PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-037750

(43)Date of publication of application : 10.02.1994

(51)Int.Cl. H04L 9/06
H04L 9/14
G09C 1/00
H04L 12/28

(21)Application number : 04-191893

(22)Date of filing : 20.07.1992

(71)Applicant : HITACHI LTD

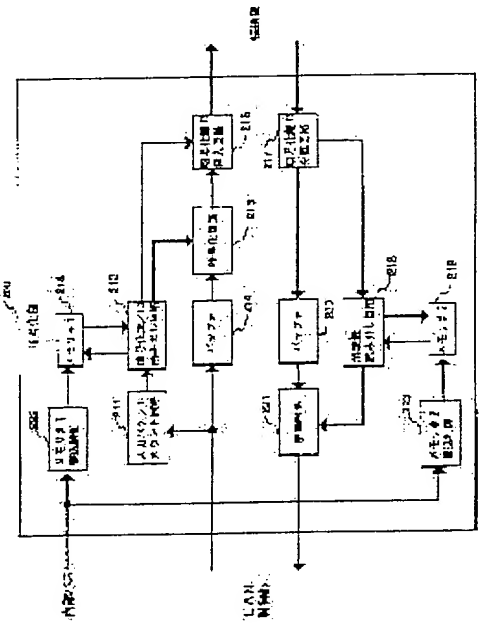
(72)Inventor : ONO MASAFUMI
TAKIYASU YOSHIHIRO
ISHIDO TOMOAKI
SUZUKI HIDEYA

(54) INFORMATION TRANSFER SYSTEM

(57)Abstract:

PURPOSE: To decode ciphered information accurately even in ciphering communication using plural ciphering keys by transferring an identification number representing definitely a ciphered key/-decoding key together with ciphered information.

CONSTITUTION: An input packet count circuit 211 in a ciphering section 200 counts number of packets inputted from a LAN control section and transfers a count to a ciphering key/ID read circuit 212. Then the ciphering key/ID read circuit 212 reads a ciphering key identifier definitely representing the ciphering key used for ciphering a packet from a memory 213. That is, a means transferring the ciphering key together with ciphering information informs the ciphering key attended with the ciphering information to a reception terminal equipment. Then a means deciding a decoding key from the ciphering key in the received information in the reception terminal equipment decides a decoding key corresponding to the ciphering key used by the transmission terminal equipment.



LEGAL STATUS

[Date of request for examination] 09.04.1999

[Date of sending the examiner's decision of rejection] 22.04.2003

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]
[Claim 1] It is the information transfer method characterized by to transmit an encryption key with encryption information in the information transfer method which enciphers and transmits information to an accepting station from a transmit terminal whenever said transmit terminal transmits encryption information, and for said accepting station to possess a means to determine a decode key from the encryption key in the received information, and to decode said receipt information using said decode key.
[Claim 2] In the information transfer method which enciphers and transmits information to an accepting station from a transmit terminal Said transmit terminal possesses a means to change the encryption key used according to a predetermined regulation. It is the information transfer method characterized by transmitting said encryption key with encryption information whenever it changes said encryption key, and for said accepting station possessing a means to determine a decode key from said encryption key in the received information, and decoding said receipt information using said decode key.
[Claim 3] The information transfer method which enciphers an encryption key at least in claims 1 or 2 using said encryption key which can decode all the communication terminals in a network.
[Claim 4] It is the information transfer method transmitted without enciphering an encryption key at least in claims 1 or 2.
[Claim 5] It is the information transfer method which it transmits the decode key corresponding to an encryption key with said encryption information in the information transfer method which enciphers and transmits information to an accepting station from a transmit terminal whenever said transmit terminal transmits encryption information, and is characterized by said accepting station decoding said receipt information using the decode key in the received information.
[Claim 6] It is the information-transfer method which said transmit terminal possesses a means change the encryption key used according to a predetermined regulation, it transmits the decode key corresponding to said encryption key with encryption information in the information-transfer method which enciphers and transmits information to an accepting station from a transmit terminal whenever it changes said encryption key, and is characterized by for said accepting station to decode said receipt information using the decode key in the received information.
[Claim 7] The information transfer method which enciphers said decode key at least in claims 5 or 6 using a common key.
[Claim 8] It is the information transfer method transmitted without enciphering said decode key at least in claims 5 or 6.
[Claim 9] In the information transfer method which enciphers and transmits information to an accepting station from a transmit terminal Said transmit terminal possesses a means to determine the encryption key identifier which shows the encryption key to be used to a meaning. It is the information transfer method characterized by transmitting said encryption key identifier with encryption information whenever it transmits encryption information, and for said accepting station possessing a means to determine a decode key from the encryption key identifier in the received information, and decoding said receipt information using said decode key.
[Claim 10] In the information transfer method which enciphers and transmits information to an accepting station from a transmit terminal A means to determine the encryption key identifier which shows the encryption key which said transmit terminal uses to a meaning, A means to change said encryption key used according to a predetermined regulation is provided. It is the information transfer method characterized by transmitting said encryption key identifier with encryption information whenever it changes said encryption key, and for said accepting station possessing a means to determine a decode key from the identifier of said encryption key in the received information, and decoding said receipt information using said decode key.
[Claim 11] The information transfer method possessing a means to associate and memorize said one or more encryption keys and said one encryption key identifier as a means to determine said encryption key identifier, in claims 9 or 10.
[Claim 12] The information transfer method which enciphers said encryption key identifier at least in claims 9, 10, or 11 using said common key.
[Claim 13] It is the information transfer method transmitted without enciphering said encryption key identifier at least in claims 9, 10, or 11.
[Claim 14] In the information transfer method which enciphers and transmits information to an accepting station

from a transmit terminal Said transmit terminal possesses a means to determine the decode key identifier which shows the decode key corresponding to the encryption key to be used to a meaning. It is the information transfer method characterized by transmitting said decode key identifier with said encryption information whenever it transmits encryption information, and for said accepting station possessing a means to determine said decode key from said decode key identifier in the received information, and decoding said receipt information using said decode key.

[Claim 15] In the information transfer method which enciphers and transmits information to an accepting station from a transmit terminal A means to determine the decode key identifier which shows the decode key corresponding to the encryption key which said transmit terminal uses to a meaning, A means to change said encryption key used according to a predetermined regulation is provided. It is the information transfer method characterized by transmitting said decode key identifier with encryption information whenever it changes said encryption key, and for said accepting station possessing a means to determine said decode key from said decode key identifier in the received information, and decoding said receipt information using said decode key.

[Claim 16] The information transfer method possessing a means to associate and memorize said one or more encryption keys and said one decode key identifier as a means to determine said decode key identifier, in claims 14 or 15.

[Claim 17] The information transfer method which enciphers said decode key identifier at least in claims 14, 15, or 16 using said common key.

[Claim 18] It is the information transfer method transmitted without enciphering said decode key identifier at least in claims 14, 15, or 16.

[Claim 19] It is the information transfer method characterized by enciphering information from a transmit terminal to an accepting station, for said transmit terminal enciphering information in the information transfer method which packet-izes encryption information and transmits it using two or more kinds of encryption keys, assembling a packet, and transmitting to said accepting station.

[Claim 20] It is the information-transfer method which said transmit terminal possesses a means determine said encryption key identifier which shows said encryption key to be used to a meaning, it transmits said encryption key identifier with said encryption information in claim 19 whenever it transmits said encryption information, said accepting station possesses a means determine said decode key from said encryption key identifier in the received information, and decodes said receipt information using said decode key.

[Claim 21] It is the information transfer method which said transmit terminal determines an encryption key from the transmit-terminal address, the accepting-station address, or both in the information transfer method which enciphers and transmits information to an accepting station from a transmit terminal, and is characterized by said accepting station determining a decode key from said transmit-terminal address in the received information, said accepting-station address, or both.

[Claim 22] The information transfer method which possesses a means to associate and memorize said one or more transmit-terminal addresses and said one encryption key as a means to determine said encryption key, in claim 21, and possesses a means to associate and memorize said one or more transmit-terminal addresses and said one decode key as a means to determine a decode key.

[Claim 23] The information transfer method which possesses a means to associate and memorize said one or more accepting-station addresses and said one encryption key as a means to determine said encryption key, in claim 21, and possesses a means to associate and memorize said one or more accepting-station addresses and said one decode key as a means to determine said decode key.

[Claim 24] A means to associate and memorize the combination of said one or more transmit-terminal addresses and said accepting-station address and said one encryption key as a means to determine said encryption key, in claim 21 is provided. The information transfer method possessing a means to associate and memorize the combination of said one or more transmit-terminal addresses and said accepting-station address, and said one decode key as a means to determine said decode key.

[Claim 25] It is the information transfer method transmitted with said transfer information, without said transmit terminal enciphering either of said transmit-terminal addresses and said accepting-station addresses, or both at least in claims 21, 22, 23, or 24.

[Claim 26] It is the information transfer method which said transmit terminal enciphers either of said transmit-terminal addresses and said accepting-station addresses, or both in claims 21, 22, 23, or 24 using a common key, and transmits with said transfer information.

[Claim 27] It is the information transfer method which said transmit terminal determines an encryption key in the information transfer method which enciphers and transmits information to an accepting station from a transmit terminal from the root information which shows the transfer path from said transmit terminal to said accepting station, and is characterized by said accepting station determining a decode key from said root information in the received information.

[Claim 28] The information transfer method which possesses a means to associate and memorize one or more root information and said one encryption key, and possesses a means to associate and memorize said one or more root information and said one decode key as a means to determine a decode key, as a means to determine said encryption key, in claim 27.

[Claim 29] It is the information transfer method transmitted with said transfer information, without said transmit terminal enciphering said root information at least in claims 27 or 28.

[Claim 30] It is the information transfer method which said transmit terminal enciphers said root information in

claims 27 or 28 using said common key at least, and transmits with said transfer information.
[Claim 31] The information-transmission method characterized by setting up an encryption key with at least one means among the command input from loading, loading from a read only memory, communication terminal, or control terminal from a floppy disk in the information transfer method which enciphers and transmits information to an accepting station from a transmit terminal.
[Claim 32] The information transfer method characterized by having two or more setting means of arbitration among the command input from loading, loading from a read only memory, communication terminal, or control terminal from a floppy disk, and choosing the setting means of arbitration further in the information transfer method which enciphers and transmits information to an accepting station from a transmit terminal.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application] This invention relates to the information transfer method which enciphers and transmits information to a receiving-side communication terminal (an accepting station is called hereafter) from a transmitting-side communication terminal (a transmit terminal is called hereafter), and relates to the information transfer method which enciphers and transmits information using the encryption algorithm (an encryption key is called hereafter) which changes with transmission places of transfer information especially.
[0002]
[Description of the Prior Art] As a conventional secrecy communication mode using a code, the technique of an indication is in JP,3-262227,A.
[0003] With the above-mentioned conventional technique, in order to perform a secrecy communication link among [of two] the Communication Bureau, the password / code memory which memorized many password codes and code codes (encryption key) to the same address to both Communication Bureau are provided. A sending station transmits the response demand signal which specified the address of a password / code memory to the receiving station, and a receiving station reads the password code memorized to the specified address, puts a password code on a reply signal, and answers a sending station. A sending station reads the code code of this address, after checking that the password code of a reply signal is right, and after it enciphers information using a code code, it transmits it to a receiving station. On the other hand, a receiving station reads the code code of the address and decodes receipt information using a code code.
[0004]
[Problem(s) to be Solved by the Invention] In applying the above-mentioned conventional technique to a connectionless communication link (CL communication link is called hereafter) like a Local Area Network (LAN is called hereafter), the following troubles arise.
[0005] First, since there is no initiation of a clear communication link in CL communication link, there is a trouble that a code code cannot be transmitted in advance of a secrecy communication link. On the other hand, although the method of using a single code code can be considered, since the danger that a third person will gain a code code and the information in a network will come to hand without notice becomes high when a single code code is used, it is not desirable.
[0006] Although what is necessary is just to use the code code of plurality [raise / network security], since a code code cannot be notified in advance of a communication link as mentioned above in CL communication link, the following new troubles occur. That is, it is not not necessarily the information addressed to itself that each terminal in a network receives in CL communication link. That is, each terminal supervises the transfer information on a network, and based on the root information included in transfer information (packet), a packet judges whether it is addressing to itself, and it selects a packet. Here, when the root information from which plurality differs using the encryption code from which plurality differs in a network is enciphered, it is possible that the same encryption root information generates from different root information. That is, if a code code is not made in agreement in such a case between sender receiver terminals, it will receive accidentally [information / which originally is not received].
[0007] As a code code is notified as a similar technique of the conventional technique at the time (for example, opening hour) of the arbitration of CL communication link, even if it makes it not generate only different encryption root information, the following troubles arise from different root information further. Namely, since it determines as mentioned above whether choice of the packet on a network receives a packet in CL communication link, an accepting station must decode a packet using all code codes for every packet reception. This not only causes [of a network throughput] a fall, but causes [of a hard amount] an increment.
[0008] The purpose of this invention is in the information transfer method using two or more encryption codes (encryption key) to offer the information transfer method which prevents the fall of the throughput accompanying incorrect reception and this of encryption information, and the increment in a hard amount, in order to maintain the confidentiality of the information transfer between sender receiver terminals.
[0009]
[Means for Solving the Problem] A means to form a means to transmit an encryption key with encryption information in a transmit terminal as first means to solve said technical problem, and to determine a decode key from the encryption key in the received information is formed in an accepting station.
[0010] The means which forms a means to transmit the decode key corresponding to an encryption key with

encryption information as second means to solve said technical problem in a transmit terminal, and reads the decode key in the received information is formed in an accepting station.
[0011] A means to form a means to determine the encryption key identifier which shows the encryption key to be used to a meaning as third means to solve said technical problem, and a means to transmit said encryption key identifier with encryption information in a transmit terminal, and to determine a decode key from the encryption key identifier in the received information is formed in an accepting station.
[0012] A means to form a means to determine the decode key identifier which shows the decode key corresponding to the encryption key to be used to a meaning as fourth means to solve said technical problem, and a means to transmit said decode key identifier with encryption information in a transmit terminal, and to determine a decode key from the decode key identifier in the received information is formed in an accepting station.
[0013] A means to form a means to determine an encryption key from the transmit-terminal address, the accepting-station address, or both in a transmit terminal as fifth means to solve said technical problem, and to determine a decode key from the transmit-terminal address in the received information, the accepting-station address, or both is formed in an accepting station.
[0014] A means to form a means to determine an encryption key from root information in a transmit terminal as sixth means to solve said technical problem, and to determine a decode key from the root information in the received information is formed in an accepting station.
[0015]
[Function] By the information transfer method using the first solution means, a means to transmit an encryption key with encryption information enables it to notify an encryption key to an accepting station along with encryption information. Furthermore, an accepting station can determine the decode key corresponding to the encryption key which the transmit terminal used with a means to determine a decode key from the encryption key in the received information. Since encryption information and an encryption key become a pair, and are transmitted by this information transfer method and a decode key can be further determined from an encryption key, even when using two or more encryption keys, it becomes possible to decode encryption information correctly.
[0016] By the information transfer method using the second solution means, a means to transmit the decode key corresponding to an encryption key with encryption information enables it to notify a decode key to an accepting station along with encryption information. Furthermore, an accepting station can determine the decode key corresponding to the encryption key which the transmit terminal used with the means which reads the decode key in the received information. Since a corresponding decode key serves as encryption information to a pair by this information transfer method and it is transmitted, even when using two or more encryption keys, it becomes possible to decode encryption information correctly.
[0017] By the information transfer method using the third solution means, a means to transmit the encryption key identifier which shows the encryption key to be used to a meaning with encryption information enables it to notify an encryption key identifier to an accepting station. Furthermore, the encryption key / decode key of a lot become settled from an encryption key identifier to an encryption key identifier with a means to determine a decode key. Since encryption information and an encryption key identifier become a pair and are transmitted by this information transfer method, even when using two or more encryption keys, it becomes possible to decode encryption information correctly.
[0018] By the information transfer method using the fourth solution means, a means to transmit the decode key identifier which shows the decode key corresponding to the encryption key to be used to a meaning with encryption information enables it to notify a decode key identifier to an accepting station. Furthermore, the encryption key / decode key of a lot become settled from a decode key identifier to a decode key identifier with a means to determine a decode key. Since encryption information and a decode key identifier become a pair and are transmitted by this information transfer method, even when using two or more encryption keys, it becomes possible to decode encryption information correctly.
[0019] By the information transfer method using the fifth solution means, the encryption key / decode key of a lot become settled with a means to determine a decode key, to the address of the transmit-terminal address, the accepting-station address, or both from a means to determine an encryption key from the transmit-terminal address, the accepting-station address, or both, the transmit-terminal address in the received information, the accepting-station address, or both. Since the transmit-terminal address and the accepting-station address are transmitted with encryption information by this information transfer method, even when using two or more encryption keys, encryption information can be decoded correctly.
[0020] By the information transfer method using the sixth solution means, the encryption key / decode key of a lot become settled to root information with a means to determine an encryption key from root information, and a means to determine a decode key from the root information in the received information. Since root information is transmitted with encryption information by this information transfer method, even when using two or more encryption keys, encryption information can be decoded correctly.
[0021]
[Example] Drawing 2 is the block diagram of the workstation (WS is called hereafter) body 100 equipped with LAN interface board 140 (a LAN interface is called hereafter) which used this invention.
[0022] In drawing 2 , user I/O interface 110, CPU120, memory 130, the LAN interface 140, and the FD control section 150 are connected with the internal bus 160. User I/O interface 110 is an interface of the WS body 100, an input device (keyboard), and an output unit (display), and has functions, such as a transfer to the internal bus 160 of

the input signal from a keyboard, and an output to the display of the signal from an internal bus 160. In addition, in this example, although the input device was used as the keyboard and the output unit was used as the display, this configuration does not limit this invention.

[0023] CPU120 is a block which performs the processing of the information from the end of the other end etc. and the control of each functional block which are inputted through the information inputted from a keyboard, and the LAN interface 140. Memory 130 is functional block which stores the various above-mentioned information, and, in the case of the processor limited of CPU120, the output waiting to a display, etc., stores the information concerned. The LAN interface 140 is a block which has a function for connecting WS to a network (LAN), and it performs encryption of the termination of a MAC (Media Access Control) layer, and transfer information while it changes a transmission format of an internal bus 160, and a transmission format of LAN. The FD control section 150 has functions, such as save in loading from a floppy disk (henceforth, FD), and FD, according to directions of CPU120. An internal bus 160 consists of a data bus to which the data which WS processes are transmitted, and a control information bus to which the control information for controlling each functional block is transmitted.

[0024] Drawing 3 is the functional block diagram of the LAN interface 140. The LAN interface 140 consists of the bus interface 170, the LAN control section 180, ROM190, the encryption section 200, and a transmission part 210.

[0025] the bus interface 170 — logging of the information block from an internal bus 160, the transfer to the LAN control section 180 of an information block, buffering of the information block further transmitted from the LAN control section 180, and the internal bus of an information block — it changes by putting. The LAN control section 180 is a block which realizes MAC layer ability, such as generation/decomposition of a packet, and addition/deletion of a packet header. The transmit-terminal address (transmitting agency address) and the accepting-station address (destination address) are included in a packet header. The MAC Address registered into ROM190 is written in the transmitting agency address. The MAC Address registered into ROM190 is the address assigned only to WS. On the other hand, the MAC Address assigned to WS of the transmission place of a packet is written in a destination address. The MAC Address of these destinations WS is memorized as a database by the memory in the LAN control section 180. The encryption section 200 decodes the encryption information received from LAN, and transmits it to the LAN control section 180 while it enciphers information from the LAN control section 180. The information from the encryption section 200 is changed into a transmission format of LAN to connect, and a transmission part 210 transmits it to LAN. Moreover, the information transmitted from LAN is changed into the format in self-WS.

[0026] Next, the encryption section 200 is explained to a detail using drawing 1 . In drawing 1 , the input packet count circuit 211 counts the number of packets inputted from the LAN control section 180, and transmits counted value to an encryption key / ID readout circuitry 212. An encryption key / ID readout circuitry 212 reads the encryption key identifier (the encryption key ID is called hereafter) which shows the encryption key used for encryption of a packet, and an encryption key to a meaning from memory 213 based on counted value.

[0027] The example of a configuration of memory 213 is shown in drawing 4 (a). To the counted value 301 from zero to 255, the encryption key 302 is registered 256 kinds so that it may correspond to one to one, and the encryption key ID 303 from 00 to FF is making it register with each encryption key by hexadecimal display in this example. In addition, it is possible to also make the same encryption key correspond to two or more different encryption keys ID. In such a case, 256 or less kinds of encryption keys are registered to 256 kinds of counted value, and the encryption key ID. Furthermore, an encryption key / ID readout circuitry 212 transmits the encryption key ID to the encryption key ID insertion circuit 216 while transmitting an encryption key to the encryption circuit 215. A buffer 214 stores the packet which inputted only the time amount to a transfer of an encryption key from the LAN control section 180. The encryption key ID insertion circuit 216 inserts the encryption key ID transmitted to the position of a packet from the encryption key / ID readout circuitry 212.

[0028] The insertion point of the encryption key ID 504 in this example is shown in drawing 5 . A packet 500 consists of a packet header and an information field 501. In the packet header, a destination address 502 and the transmitting agency address 503 are written in. Encryption key ID 504 It inserts between User Information 505 and a packet header. In a MAC layer, since the encryption key ID 504 and User Information 505 are dealt with as an information field 501, insertion of the encryption key ID 504 does not affect a MAC layered protocol.

[0029] On the other hand, the encryption circuit 215 enciphers the packet inputted from a buffer 214, and transmits it to the encryption key ID insertion circuit 216. In this example, it enciphers using the encryption key (a common encryption key is called hereafter) which can decode all the communication equipment in a network, and the encryption key ID enciphers other parts using the encryption key according to individual read from memory 213.

[0030] Next, the processing when receiving encryption information from LAN is explained. The encryption key ID separation circuit 217 starts the section of the encryption key ID from a reception encryption packet, and transmits it to the decode key readout circuitry 218. Parts other than the encryption key ID are stored in a buffer 220 as they are. The decode key readout circuitry 218 reads a decode key from memory 219 based on the encryption key ID. Since the encryption key ID is enciphered with the common encryption key, all accepting stations can decode the encryption key ID. In addition, since the encryption key ID enciphered as the encryption key ID of a plaintext since the common encryption key was used for encryption of the encryption key ID in this example corresponds to one to one, it is also possible to use without decoding the encryption key ID of the packet which received, and to choose a decode key. Moreover, it is also possible to transmit with the encryption information on other, without enciphering the encryption key ID, and a decode key is chosen, using the encryption key ID which the encryption key ID separation circuit 217 cut down in that case as it is.

[0031] The example of a configuration of memory 219 is shown in drawing 4 (b). In this example, the decode key 402

is registered 256 kinds so that it may correspond to one to one to the encryption key ID 401 from 00 to FF by hexadecimal display. In addition, it is possible to also make the same decode key correspond to two or more different encryption keys ID like memory 213. In such a case, 256 or less kinds of decode keys are registered to 256 kinds of encryption keys ID. The decode key readout circuitry 218 reads the decode key which becomes settled uniquely with the encryption key ID, and transmits it to the decode circuit 221. The decode circuit 221 decodes the packet inputted from a buffer 220 using a decode key, and transmits it to the LAN control section 180. [0032] Next, the setting approach of of the counted value / encryption key / encryption key ID / decode key in this example is explained. In this example, setting data are loaded from a floppy disk (FD) at the time of a system construction. The memory write control 222 performs write-in control of the setting data to the memory 213 which registers counted value / encryption key / encryption key ID. On the other hand, the memory write control 223 performs write-in control of the setting data to the memory 219 which registers encryption key ID / decode key. In addition, when modification of setting data arises, the contents of registration in memory are rewritten by the command input from the communication terminal or control terminal in a network. In this case, the setting data processed by CPU120 within the WS body 100 are transmitted to the memory write control 222 and the memory write control 223 through an internal bus 160. Write control 222 and 223 rewrites the contents of registration of memory 213 and memory 219 based on directions of CPU120.

[0033] Next, the second example is explained using drawing 6 and drawing 7 . In this example, the encryption key used based on the destination address of a packet inputted from the LAN control section 180 is determined. In addition, since only actuation of the first example and the encryption section 200 differs, this example explains only the encryption section 200.

[0034] In drawing 6 , the destination address readout circuitry 224 reads the destination address of a packet inputted from the LAN control section 180, and transmits it to the encryption key readout circuitry 225. The encryption key readout circuitry 225 reads the encryption key to be used from memory 213 based on a destination address.

[0035] The example of a configuration of the memory 213 in this example is shown in drawing 7 (a). By memory 213, to 256 kinds of transmitting packet destination addresses 304 (DA#0-DA#255), the encryption key 302 is registered 256 kinds so that it may correspond to one to one. The address for the individual communication link to each terminal, the address for a group communication link given common to two or more terminals, and the address for simultaneous broadcasts given common to all terminals are located in a destination address. In addition, it is possible to also make the same encryption key correspond to two or more different destination addresses. In such a case, 256 or less kinds of encryption keys are registered to 256 kinds of destination addresses. Furthermore, it is also possible to register an encryption key to the combination of a destination address and the transmitting agency address, so that it may correspond to one to one. Furthermore, the encryption key readout circuitry 225 transmits an encryption key to the encryption circuit 215. A buffer 214 stores the packet which inputted only the time amount to a transfer of an encryption key from the LAN control section 180. The encryption circuit 215 enciphers the packet inputted from a buffer 214, and transmits it to a transmission part 210. In this example, a destination address and the transmitting agency address are enciphered using a common encryption key, and other parts are enciphered using the encryption key read from memory 213.

[0036] In this example, since a characteristic parameter like the encryption key ID in the first example is not used, the packet format delivered and received between the encryption section 200 and a transmission part 210 is in agreement with the packet format of the MAC layered protocol which a LAN control section supports.

[0037] Next, the processing when receiving encryption information (packet) from LAN is explained. The destination address separation circuit 226 copies the section of a destination address from an encryption packet, and transmits it to the decode key readout circuitry 218. The decode key readout circuitry 218 reads a decode key from memory 219 based on a destination address. Since the destination address is enciphered with the common encryption key, all accepting stations can decode a destination address. In addition, since the common encryption key is used for encryption of a destination address in this example and the destination address enciphered as the destination address of a plaintext corresponds to one to one, it is also possible to use without decoding the destination address of the packet which received, and to choose a decode key. Moreover, it is also possible to transmit with the encryption information on other, without enciphering a destination address, and a decode key is chosen, using the destination address which the destination address separation circuit 226 copied in that case as it is.

[0038] The example of a configuration of memory 219 is shown in drawing 7 (b). In this example, it is registered so that the decode key 402 of a class (N+2) may correspond to one to one to the destination address 403 of the receive packet of a class (N+2). To the address of the total (N+2) class of one kind of simultaneous multiple address address in the case of performing broadcast to the group address N class in case of performing the group communication link to the group who specifically contains one kind of self-address in case self-WS serves as an accepting station of an individual communication link, and self-WS, and all terminals, the decode key 402 of a class is registered so that it may correspond to one to one (N+2). In addition, it is possible to also make the same decode key correspond to two or more different receive-packet destination addresses. In such a case, (N+2) the decode key below a class (N+2) is registered to the destination address of a class. Furthermore, it is also possible to register a decode key to the combination of a destination address and the sending agency address, so that it may correspond to one to one. The decode key readout circuitry 218 reads the decode key which becomes settled uniquely with a destination address, and transmits it to the decode circuit 221. The decode circuit 221 decodes the packet inputted from a buffer 220 using a decode key, and transmits it to the LAN control section 180.

[0039] Next, the setting approach of of the transmitting packet destination address / encryption key in this example, and a receive-packet destination address / decode key is explained. In this example, setting data are loaded from FD at the time of a system construction. The memory write control 222 performs write-in control of the setting data to the memory 213 which registers a transmitting packet destination address / encryption key. On the other hand, memory #2 write control 223 performs write-in control of the setting data to the memory 219 which registers a receive-packet destination address / decode key. In addition, when modification of setting data arises, the contents of registration in memory are rewritten by the command input from the communication terminal or control terminal in a network. In this case, the setting data processed by CPU120 within the WS body 100 are transmitted to the memory write control 222 and the memory write control 223 through an internal bus 160. Write control 222,223 rewrites the contents of registration of memory 213 and memory 219 according to directions of CPU120.
[0040] Next, the third example is explained using drawing 8 and drawing 9 . In this example, the encryption key used based on the root information on the packet inputted from the LAN control section 180 is determined. In addition, since the first example of the above-mentioned [this example] differs only from actuation of the encryption section 200, only the encryption section 200 is explained.
[0041] In drawing 8 , the root information readout circuitry 227 reads the root information on the packet inputted from the LAN control section 180, and transmits it to the encryption key readout circuitry 225. The encryption key readout circuitry 225 reads the encryption key to be used from memory 213 based on root information.
[0042] The example of a configuration of the memory 213 in this example is shown in drawing 9 (a). By memory 213, to 256 kinds of transmitting packet root information 305 (VCN#0-VCN#255), the encryption key 302 is registered 256 kinds so that it may correspond to one to one. In addition, the setting approach of root information is arbitrary and does not restrict this invention. The encryption key readout circuitry 225 transmits an encryption key to the encryption circuit 215. A buffer 214 stores the packet which inputted only the time amount to a transfer of said encryption key from the LAN control section 180. The encryption circuit 215 enciphers the packet inputted from a buffer 214, and transmits it to a transmission part 210. In this example, root information is enciphered using a common encryption key, and other parts are enciphered using the encryption key read from memory 213.
[0043] Since a characteristic parameter [like the encryption key ID in the first example] whose this example is also is not used, the packet format delivered and received between the encryption section 200 and a transmission part 210 is completely in agreement with the packet format of the MAC layered protocol which a LAN control section supports.
[0044] Next, the processing when receiving encryption information (packet) from LAN is explained. The root information-separator circuit 228 copies the section of root information from an encryption packet, and transmits it to the decode key readout circuitry 218. The decode key readout circuitry 218 reads a decode key from memory 219 based on root information. Since root information is enciphered with the common encryption key, all accepting stations can decode root information. In addition, since the root information enciphered as the root information on a plaintext since the common encryption key was used for encryption of root information in this example corresponds to one to one, it uses without decoding the root information on the packet which received, and it can also choose a decode key. Moreover, it is also possible to transmit with the encryption information on other, without enciphering root information, and a decode key is chosen, using the root information which the root information-separator circuit 228 copied in that case as it is.
[0045] The example of a configuration of memory 219 is shown in drawing 9 (b). In this example, to the root information 404 on a receive packet, 256 kinds of decode keys 402 are registered so that it may correspond to one to one. In addition, it is possible to also make the same decode key correspond to two or more different root information. In such a case, 256 or less kinds of decode keys are registered to 256 kinds of root information. The decode key readout circuitry 218 reads the decode key which becomes settled uniquely for root information, and transmits it to the decode circuit 221. The decode circuit 221 decodes the packet inputted from a buffer 220 using a decode key, and transmits it to the LAN control section 180.
[0046] Next, the setting approach of of the transmitting packet root information / encryption key in this example, and a receive-packet root information / decode key is explained. In this example, setting data are loaded from FD at the time of a system construction. The write control 222 of memory 213 performs write-in control of the setting data to the memory 213 which registers transmitting packet root information / encryption key. On the other hand, the write control 223 of memory 219 performs write-in control of the setting data to the memory 219 which registers receive-packet root information / decode key. In addition, when modification of setting data arises, the contents of registration in memory are rewritten by the command input from the communication terminal or control terminal in a network. In this case, the setting data processed by CPU120 within the WS body 100 are transmitted to memory #1 write control 222 and memory #2 write control 223 through an internal bus 160. Write control 222 and 223 rewrites the contents of registration of memory 213 and memory 219 based on directions of CPU120.
[0047] Next, the fourth example is explained using drawing 10 and drawing 11 . In this example, the encryption key used based on the MAC Address of the communication terminal which transmits a packet is determined. Therefore, when one communication terminal has two or more MAC Addresses physically, the end of an end will have two or more encryption keys, and when two or more communication terminals share one MAC Address, two or more terminals will share one encryption key. In addition, since the first example of the above-mentioned [this example] differs only from actuation of the encryption section 200, only the encryption section 200 is explained.
[0048] In drawing 10 , the transmitting agency address readout circuitry 229 reads the transmitting agency address of the packet inputted from the LAN control section 180, and transmits it to the encryption key readout circuitry

225. The encryption key readout circuitry 225 reads the encryption key to be used from memory 213 based on the said transmitting former address.
[0049] The example of a configuration of the memory 213 in this example is shown in drawing 11 (a). In this example, one kind of encryption key 302 is registered to the 1 kind of transmitting packet transmitting former addresses 306. The encryption key readout circuitry 225 transmits an encryption key to the encryption circuit 215. A buffer 214 stores the packet which inputted only the time amount to a transfer of an encryption key from the LAN control section 180. The encryption circuit 215 enciphers the packet inputted from a buffer 214, and transmits it to a transmission part 210. In this example, a destination address and the transmitting agency address are enciphered using a common encryption key, and other parts are enciphered using the encryption key read from memory 213.
[0050] Since a characteristic parameter [like the encryption key ID in the first example] whose this example is also is not used, the packet format delivered and received between the encryption section 200 and a transmission part 210 is in agreement with the packet format of the MAC layered protocol which a LAN control section supports.
[0051] Next, the processing when receiving encryption information (packet) from LAN is explained. The transmitting agency address separation circuit 230 copies the section of the transmitting agency address from an encryption packet, and transmits it to the decode key readout circuitry 218. The decode key readout circuitry 218 reads a decode key from memory 219 based on the transmitting agency address. Since the transmitting agency address is enciphered with the common encryption key, all accepting stations can decode the transmitting agency address. In addition, since the common encryption key is used for encryption of the transmitting agency address in this example and the transmitting agency address enciphered as the transmitting agency address of a plaintext corresponds to one to one, it is also possible to use without decoding the transmitting agency address of the packet which received, and to choose a decode key. Moreover, it is also possible to transmit with the encryption information on other, without enciphering the transmitting agency address, and a decode key is chosen, using the transmitting agency address which the transmitting agency address separation circuit 230 copied in that case as it is.
[0052] The example of a configuration of memory 219 is shown in drawing 11 (b). In this example, it is registered so that 256 kinds of decode keys 402 may correspond to one to one to the transmitting agency address 405 of 256 kinds of receive packets. In addition, it is possible to also make the same decode key correspond to two or more different receive-packet transmitting former addresses. In such a case, 256 or less kinds of decode keys are registered to 256 kinds of destination addresses. The decode key readout circuitry 218 reads the decode key which becomes settled uniquely in the transmitting agency address, and transmits it to the decode circuit 221. The decode circuit 221 decodes the packet inputted from a buffer 220 using a decode key, and transmits it to the LAN control section 180.
[0053] Next, the setting approach of of the transmitting packet transmitting former address / encryption key in this example, and the receive-packet transmitting former address / decode key is explained. In this example, setting data are loaded from FD at the time of a system construction. Memory 213 write control 222 performs write-in control of the setting data to the memory 213 which registers the transmitting packet transmitting former address / encryption key. On the other hand, the write control 223 of memory 219 performs write-in control of the setting data to the memory 219 which registers the receive-packet transmitting former address / decode key. In addition, when modification of setting data arises, the contents of registration in memory are rewritten by the command input from the communication terminal or control terminal in a network. In this case, the setting data processed by CPU120 within the WS body 100 are transmitted to the write control 222 of memory 213, and the write control 223 of memory 219 through an internal bus 160. Write control 222 and 223 rewrites the contents of registration of memory 213 and memory 219 based on directions of CPU120.
[0054] Next, the fifth example is explained using drawing 12 , drawing 13 , and 14. This example transmits an encryption key with encryption information to the first example transmitting the encryption key ID with encryption information. In addition, since only actuation of the first example and the encryption section 200 differs, this example also explains only the encryption section 200.
[0055] In drawing 12 , the input packet count circuit 211 counts the number of packets inputted from the LAN control section 180, and transmits counted value to the encryption key readout circuitry 231. The encryption key readout circuitry 231 reads the encryption key used for encryption of a packet from memory 213 based on counted value.
[0056] The example of a configuration of memory 213 is shown in drawing 13 (a). In this example, to the counted value 301 from zero to 255, the encryption key 302 is registered 256 kinds so that it may correspond to one to one. In addition, it is possible to also make the same encryption key correspond to two or more different counted value. In such a case, 256 or less kinds of encryption keys are registered to 256 kinds of counted value. Furthermore, the encryption key readout circuitry 231 transmits an encryption key to the encryption circuit 215 and the encryption key insertion circuit 232. A buffer 214 stores the packet which inputted only the time amount to a transfer of an encryption key from the LAN control section 180. The encryption key insertion circuit 232 inserts the encryption key transmitted to the position of a packet from the encryption key readout circuitry 231.
[0057] The insertion point of the encryption key 506 in this example is shown in drawing 14 . A packet 500 consists of a packet header and an information field 501. In the packet header, a destination address 502 and the transmitting agency address 503 are written in. The encryption key 506 is inserted between User Information 505 and a packet header. In a MAC layer, since the encryption key 506 and User Information 505 are dealt with as an information field 501, insertion of the encryption key 506 does not affect a MAC layered protocol.
[0058] On the other hand, the encryption circuit 215 enciphers the packet inputted from a buffer 214, and transmits

it to the encryption key insertion circuit 232. In this example, an encryption key is enciphered using the encryption key (a common encryption key is called hereafter) which can decode all the communication equipment in a network, and other parts are enciphered using the encryption key according to individual read from memory 213.
[0059] Next, the processing when receiving encryption information from LAN is explained. The encryption key separation circuit 233 starts the section of an encryption key from a reception encryption packet, and transmits it to the decode key readout circuitry 218. Parts other than an encryption key are stored in a buffer 220 as they are. The decode key readout circuitry 218 reads a decode key from memory 219 based on an encryption key. Since the encryption key is enciphered with the common encryption key, all accepting stations can decode an encryption key. In addition, since the common encryption key is used for encryption of an encryption key in this example and the encryption key enciphered as the encryption key of a plaintext corresponds to one to one, it is also possible to use without decoding the encryption key of the packet which received, and to choose a decode key. Moreover, it is also possible to transmit with the encryption information on other, without enciphering an encryption key, and a decode key is chosen, using the encryption key which the encryption key separation circuit 233 cut down in that case as it is.
[0060] The example of a configuration of memory 219 is shown in drawing 13 (b). In this example, the decode key 402 (D-Key#0-D-Key#255) is registered 256 kinds so that it may correspond to 256 kinds of encryption keys 406 (C-Key#0-C-Key#255) at one to one. The decode key readout circuitry 218 reads the decode key which becomes settled uniquely with an encryption key, and transmits it to the decode circuit 221. The decode circuit 221 decodes the packet inputted from a buffer 220 using a decode key, and transmits it to the LAN control section 180.
[0061] Next, the setting approach of of the counted value / encryption key / decode key in this example is explained. In this example, setting data are loaded from a floppy disk (FD) at the time of a system construction. Memory #1 write control 222 performs write-in control of the setting data to the memory 213 which registers counted value / encryption key. On the other hand, the write control 223 of memory 219 performs write-in control of the setting data to the memory 219 which registers an encryption key / decode key. In addition, when modification of setting data arises, the contents of registration in memory are rewritten by the command input from the communication terminal or control terminal in a network. In this case, the setting data processed by CPU120 within the WS body 100 are transmitted to the write control 222 of memory 213, and the write control 223 of memory 219 through an internal bus 160. Write control 222 and 223 rewrites the contents of registration of memory 213 and memory 219 based on directions of CPU120.
[0062] Next, the sixth example is explained using drawing 15 , drawing 16 , and drawing 17 . This example transmits a decode key with encryption information to the first example transmitting the encryption key ID with encryption information. In addition, since only actuation of the first example and the encryption section 200 differs, this example also explains only the encryption section 200.
[0063] In drawing 15 , the input packet count circuit 211 counts the number of packets inputted from the LAN control section 180, and transmits counted value to an encryption key / decode key readout circuitry 234. An encryption key / decode key readout circuitry 234 reads the decode key used at the time of the encryption key used for encryption of a packet, and decode from memory 213 based on counted value.
[0064] The example of a configuration of memory 213 is shown in drawing 16 . In this example, to the counted value 301 from zero to 255, the encryption key 302 and the decode key 307 are registered 256 sets so that it may correspond to one to one. In addition, it is possible to also make the same encryption key / decode key correspond to two or more different counted value. In such a case, 256 or less sets of an encryption key / decode keys are registered to 256 kinds of counted value. Furthermore, an encryption key / decode key readout circuitry 234 transmits a decode key to the decode key insertion circuit 235 while transmitting an encryption key to the encryption circuit 215. A buffer 214 stores the packet which inputted only the time amount to a transfer of an encryption key from the LAN control section 180. The decode key insertion circuit 232 inserts the decode key transmitted to the position of a packet from the encryption key / decode key readout circuitry 234.
[0065] The insertion point of the decode key 507 in this example is shown in drawing 17 . A packet 500 consists of a packet header and an information field 501. In the packet header, a destination address 502 and the transmitting agency address 503 are written in. The decode key 507 is inserted between User Information 505 and a packet header. In a MAC layer, since the decode key 507 and User Information 505 are dealt with as an information field 501, insertion of the decode key 507 does not affect a MAC layered protocol.
[0066] The encryption circuit 215 enciphers the packet inputted from a buffer 214, and transmits it to the decode key insertion circuit 235. In this example, a decode key is enciphered using a common encryption key, and other parts are enciphered using the encryption key according to individual read from memory 213.
[0067] Next, the processing when receiving encryption information from LAN is explained. The decode key separation circuit 236 starts the section of a decode key from a reception encryption packet, and transmits it to the decode circuit 221. Since the decode key is enciphered with the common encryption key, all accepting stations can decode a decode key. Moreover, it is also possible to transmit with the encryption information on other, without enciphering a decode key, and the decode key which the decode key separation circuit 236 cut down in that case is used as it is. The decode circuit 221 decodes the packet transmitted from the decode key separation circuit 236 using the decode key concerned, and transmits it to the LAN control section 180.
[0068] Next, the setting approach of of the counted value / encryption key / decode key in this example is explained. In this example, setting data are loaded from a floppy disk (FD) at the time of a system construction. The write control 222 of memory 213 performs write-in control of the setting data to the memory 213 which registers

counted value / encryption key / decode key. In addition, when modification of setting data arises, the contents of registration in memory are rewritten by the command input from the communication terminal or control terminal in a network. In this case, the setting data processed by CPU120 within the WS body 100 are transmitted to the write control 222 of memory 213 through an internal bus 160. Write control 222 rewrites the contents of registration of memory 213 based on directions of CPU120.

[0069] Next, the seventh example is explained using drawing 18 , drawing 19 , and 20. This example transmits a decode key identifier (the decode key ID is called hereafter) with encryption information to the first example transmitting the encryption key ID with encryption information. In addition, since only actuation of the first example and the encryption section 200 differs, this example also explains only the encryption section 200.

[0070] In drawing 18 , the input packet count circuit 211 counts the number of packets inputted from the LAN control section 180, and transmits counted value to an encryption key / ID readout circuitry 212. An encryption key / ID readout circuitry 212 reads the decode key ID which shows the decode key corresponding to the encryption key and encryption key which are used for encryption of a packet to a meaning from memory 213 based on counted value.

[0071] The example of a configuration of memory 213 is shown in drawing 19 (a). In this example, to the counted value 301 from zero to 255, the encryption key 302 and the decode key ID 308 are registered 256 sets so that it may correspond to one to one. In addition, it is possible to also make same encryption key / decode key ID correspond to two or more different counted value. In such a case, 256 or less sets of an encryption key / decode keys ID are registered to 256 kinds of counted value. Furthermore, an encryption key / decode key readout circuitry 212 transmits the decode key ID to the decode key ID insertion circuit 237 while transmitting an encryption key to the encryption circuit 215. A buffer 214 stores the packet which inputted only the time amount to a transfer of an encryption key from the LAN control section 180. The decode key ID insertion circuit 237 inserts the decode key ID transmitted to the position of a packet from the encryption key / ID readout circuitry 212.

[0072] The insertion point of the decode key ID 508 in this example is shown in drawing 20 . A packet 500 consists of a packet header and an information field 501. In the packet header, a destination address 502 and the transmitting agency address 503 are written in. The decode key ID 508 is inserted between User Information 505 and a packet header. In a MAC layer, since the decode key ID 508 and User Information 505 are dealt with as an information field 501, insertion of the decode key ID 508 does not affect a MAC layered protocol.

[0073] The encryption circuit 215 enciphers the packet inputted from a buffer 214, and transmits it to the decode key ID insertion circuit 237. In this example, a decode key is enciphered using a common encryption key, and other parts are enciphered using the encryption key according to individual read from memory 213.

[0074] Next, the processing when receiving encryption information from LAN is explained. The decode key ID separation circuit 237 starts the section of the decode key ID from a reception encryption packet, and transmits it to the decode key readout circuitry 218. Parts other than the decode key ID are stored in a buffer 220 as they are. The decode key readout circuitry 218 reads a decode key from memory 219 based on said decode key ID. Since the decode key ID is enciphered with the common encryption key, all accepting stations can decode the decode key ID. In addition, since the common encryption key is used for encryption of the decode key ID in this example and the decode key ID enciphered as the decode key ID of a plaintext corresponds to one to one, it is also possible to use without decoding the decode key ID of the packet which received, and to choose a decode key. Moreover, it is also possible to transmit with the encryption information on other, without enciphering the decode key ID, and a decode key is chosen, using the decode key ID which the decode key ID separation circuit 238 cut down in that case as it is.

[0075] The example of a configuration of memory 219 is shown in drawing 19 (b). In this example, the decode key 402 is registered 256 kinds so that it may correspond to 256 kinds of decode keys ID 407 at one to one. The decode key readout circuitry 218 reads the decode key which becomes settled uniquely with the decode key ID, and transmits it to the decode circuit 221. The decode circuit 221 decodes the packet inputted from a buffer 220 using a decode key, and transmits it to the LAN control section 180.

[0076] Next, the setting approach of of the counted value / encryption key / decode key ID / decode key in this example is explained. In this example, setting data are loaded from a floppy disk (FD) at the time of a system construction. The write control 222 of memory 213 performs write-in control of the setting data to the memory 213 which registers counted value / encryption key / decode key ID. The write control 223 of memory 219 performs write-in control of the setting data to the memory 219 which registers decode key ID / decode key. In addition, when modification of setting data arises, the contents of registration in memory are rewritten by the command input from the communication terminal or control terminal in a network. In this case, the setting data processed by CPU120 within the WS body 100 are transmitted to the write control 222 of memory 213 through an internal bus 160. Write control 222 rewrites the contents of registration of memory 213 and memory 219 based on directions of CPU120.

[0077] Next, the eighth example is explained using drawing 21 and drawing 22 . As for the seventh example, the setting approaches of the first example, memory 213, and memory 219 differ. That is, in the first example, a setup of memory 213,219 was performed by carrying out loading of the setting data from FD. In this example, as shown in drawing 21 , the setting data of memory 213,219 are read from ROM191 within the LAN interface 140.

[0078] In drawing 22 , from ROM191, write control 239 reads the setting data (counted value / encryption key / encryption key ID) to memory 213, and writes them in memory 213. From ROM191, write control 240 reads the setting data (encryption key ID / decode key) to memory 219, and writes them in memory 219.

[0079] In addition, it is easy to apply this example to said the second thru/or seventh example. What is necessary is to use as a transmitting packet destination address / encryption key the contents memorized to ROM191 as an object for memory 213, and just to let them be a receive-packet destination address / decode key as an object for memory 219, in applying to the second example. What is necessary is to use as transmitting packet root information / encryption key the contents memorized to ROM191 as an object for memory 213, and just to let them be receive-packet root information / decode key as an object for memory 219, in applying to the third example. What is necessary is just to let the contents memorized to ROM191 be the receive-packet transmitting former address / decode key as an object for memory 213 as the transmitting packet transmitting former address / encryption key, and an object for memory 219, in applying to the fourth example. What is necessary is just to let the contents memorized to ROM191 be an encryption key / decode key as counted value / encryption key, and an object for memory 219 as an object for memory 213, in applying to the fifth example. What is necessary is just to let the contents memorized to ROM191 be counted value / encryption key / decode key as an object for memory 213, in applying to the sixth example. What is necessary is just to let the contents memorized to ROM191 be decode key ID / decode key as an object for memory 213 as counted value / encryption key / decode key ID, and an object for memory 219, in applying to the seventh example.

[0080]

[Effect of the Invention] Since the identification information which shows an encryption key / decode key to a meaning with encryption information is transmitted according to this invention, also in the secrecy communication link using two or more encryption keys, encryption information is correctly decipherable.

[0081] Since the encryption key of arbitration can be used to the communication terminal of arbitration when using an encryption key or the decode key itself as identification information, the dependability of a secrecy communication link improves more.

[0082] Since it is expressing the encryption key or the decode key as an identifier in addition to the ability to use the encryption key of arbitration to the communication terminal of arbitration in using an encryption key identifier or a decode key identifier as identification information, the dependability of a secrecy communication link improves further.

[0083] When using the terminal address or root information as identification information, an encryption key / decode key can be specified without using a special identifier.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] The block diagram of the encryption section in the first example of this invention.
[Drawing 2] The block diagram of the communication terminal (WS) body in the first example of this invention.
[Drawing 3] The block diagram of the LAN interface in the first example of this invention.
[Drawing 4] The explanatory view of the encryption key storage section in the first example of this invention, and the decode key storage section.
[Drawing 5] The explanatory view of the packet in the first example of this invention.
[Drawing 6] The block diagram of the encryption section in the second example of this invention.
[Drawing 7] The explanatory view of the encryption key storage section in the second example of this invention, and the decode key storage section.
[Drawing 8] The block diagram of the encryption section in the third example of this invention.
[Drawing 9] The explanatory view of the encryption key storage section in the third example of this invention, and the decode key storage section.
[Drawing 10] The block diagram of the encryption section in the fourth example of this invention.
[Drawing 11] The explanatory view of the encryption key storage section in the fourth example of this invention, and the decode key storage section.
[Drawing 12] The block diagram of the encryption section in the fifth example of this invention.
[Drawing 13] The explanatory view of the encryption key storage section in the fifth example of this invention, and the decode key storage section.
[Drawing 14] The explanatory view of the packet in the fifth example of this invention.
[Drawing 15] The block diagram of the encryption section in the sixth example of this invention.
[Drawing 16] The encryption key in the sixth example of this invention, and the explanatory view of the decode key storage section.
[Drawing 17] The explanatory view of the packet in the sixth example of this invention.
[Drawing 18] The block diagram of the encryption section in the seventh example of this invention.
[Drawing 19] The block diagram of the encryption key storage section in the seventh example of this invention, and the decode key storage section.
[Drawing 20] The explanatory view of the packet in the seventh example of this invention.
[Drawing 21] The block diagram of the LAN interface in the eighth example of this invention.
[Drawing 22] The block diagram of the encryption section in the eighth example of this invention.
[Description of Notations]
200 [— Memory, 215 / — An encryption circuit, 216 / — An encryption key ID insertion circuit, 217 / — An encryption key ID separation circuit, 218 / — A decode key readout circuitry 219 / — Memory, 221 / — A decode circuit, 222 / — Memory write control, 223 / — Memory write control.] — The encryption section, 211 — An input packet count circuit, 212 — An encryption key / ID readout circuitry, 213

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平6－37750

(43)公開日　平成６年(1994)２月10日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　9/06				
9/14				
Ｇ０９Ｃ　1/00		9194－5Ｌ		
		7117－5Ｋ	Ｈ０４Ｌ　9/02	Ｚ
		8529－5Ｋ	11/00　３１０	Ｚ

審査請求　未請求　請求項の数32(全 27 頁)　最終頁に続く

(21)出願番号　特願平4－191893

(22)出願日　平成４年(1992)７月20日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　大野　雅史
東京都国分寺市東恋ケ窪１丁目280番地
株式会社日立製作所中央研究所内

(72)発明者　滝安　美弘
東京都国分寺市東恋ケ窪１丁目280番地
株式会社日立製作所中央研究所内

(72)発明者　石藤　智昭
東京都国分寺市東恋ケ窪１丁目280番地
株式会社日立製作所中央研究所内

(74)代理人　弁理士　小川　勝男

最終頁に続く

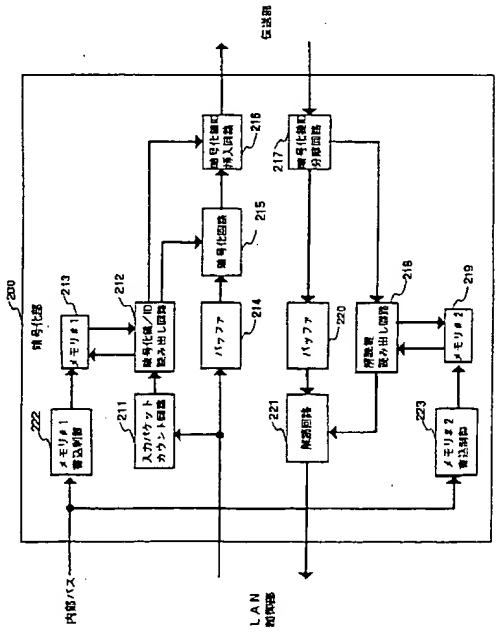
(54)【発明の名称】　情報転送方式

(57)【要約】

【構成】暗号化鍵を暗号化情報と共に転送する手段を送信端末に設け、受信した情報の中の暗号化鍵から解読鍵を決定する手段を受信端末に設ける。

【効果】暗号化情報と共に暗号化鍵／解読鍵を一意に示す情報を転送するすることで、複数の暗号化鍵を用いる秘匿通信においても受信端末に暗号化鍵／解読鍵の識別情報を随時通知することが可能になるので、暗号化情報を正確に解読することができる。

図１



1

【特許請求の範囲】

【請求項１】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は暗号化情報を転送する毎に暗号化鍵を暗号化情報と共に転送し、前記受信端末は受信した情報の中の暗号化鍵から解読鍵を決定する手段を具備し、前記解読鍵を用いて前記受信情報を解読することを特徴とする情報転送方式。

【請求項２】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は所定の規則に従って使用する暗号化鍵を変更する手段を具備し、前記暗号化鍵を変更する毎に前記暗号化鍵を暗号化情報と共に転送し、前記受信端末は受信した情報の中の前記暗号化鍵から解読鍵を決定する手段を具備し、前記解読鍵を用いて前記受信情報を解読することを特徴とする情報転送方式。

【請求項３】請求項１または２において、ネットワーク内の全ての通信端末が解読可能な前記暗号化鍵を用いて、少なくとも暗号化鍵を暗号化する情報転送方式。

【請求項４】請求項１または２において、少なくとも暗号化鍵は暗号化せずに転送する情報転送方式。

【請求項５】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は暗号化情報を転送する毎に暗号化鍵に対応する解読鍵を前記暗号化情報と共に転送し、前記受信端末は受信した情報の中の解読鍵を用いて前記受信情報を解読することを特徴とする情報転送方式。

【請求項６】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は所定の規則に従って使用する暗号化鍵を変更する手段を具備し、前記暗号化鍵を変更する毎に前記暗号化鍵に対応する解読鍵を暗号化情報と共に転送し、前記受信端末は受信した情報の中の解読鍵を用いて前記受信情報を解読することを特徴とする情報転送方式。

【請求項７】請求項５または６において、共通鍵を用いて、少なくとも前記解読鍵を暗号化する情報転送方式。

【請求項８】請求項５または６において、少なくとも前記解読鍵は暗号化せずに転送する情報転送方式。

【請求項９】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は使用する暗号化鍵を一意に示す暗号化鍵識別子を決定する手段を具備し、暗号化情報を転送する毎に前記暗号化鍵識別子を暗号化情報と共に転送し、前記受信端末は受信した情報の中の暗号化鍵識別子から解読鍵を決定する手段を具備し、前記解読鍵を用いて前記受信情報を解読することを特徴とする情報転送方式。

【請求項１０】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は使用する暗号化鍵を一意に示す暗号化鍵識別子を決定する手段と、所定の規則に従って使用する前記暗号化鍵を変更する手段を具備し、前記暗号化鍵を変更する毎に前記暗

2

号化鍵識別子を暗号化情報と共に転送し、前記受信端末は受信した情報の中の前記暗号化鍵の識別子から解読鍵を決定する手段を具備し、前記解読鍵を用いて前記受信情報を解読することを特徴とする情報転送方式。

【請求項１１】請求項９または１０において、前記暗号化鍵識別子を決定する手段として、一つあるいは複数の前記暗号化鍵と一つの前記暗号化鍵識別子を関連付けて記憶する手段を具備する情報転送方式。

【請求項１２】請求項９，１０または１１において、前記共通鍵を用いて、少なくとも前記暗号化鍵識別子を暗号化する情報転送方式。

【請求項１３】請求項９，１０または１１において、少なくとも前記暗号化鍵識別子は暗号化せずに転送する情報転送方式。

【請求項１４】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は使用する暗号化鍵に対応する解読鍵を一意に示す解読鍵識別子を決定する手段を具備し、暗号化情報を転送する毎に前記解読鍵識別子を前記暗号化情報と共に転送し、前記受信端末は受信した情報の中の前記解読鍵識別子から前記解読鍵を決定する手段を具備し、前記解読鍵を用いて前記受信情報を解読することを特徴とする情報転送方式。

【請求項１５】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は使用する暗号化鍵に対応する解読鍵を一意に示す解読鍵識別子を決定する手段と、所定の規則に従って使用する前記暗号化鍵を変更する手段を具備し、前記暗号化鍵を変更する毎に前記解読鍵識別子を暗号化情報と共に転送し、前記受信端末は受信した情報の中の前記解読鍵識別子から前記解読鍵を決定する手段を具備し、前記解読鍵を用いて前記受信情報を解読することを特徴とする情報転送方式。

【請求項１６】請求項１４または１５において、前記解読鍵識別子を決定する手段として、一つあるいは複数の前記暗号化鍵と一つの前記解読鍵識別子を関連付けて記憶する手段を具備する情報転送方式。

【請求項１７】請求項１４，１５または１６において、前記共通鍵を用いて、少なくとも前記解読鍵識別子を暗号化する情報転送方式。

【請求項１８】請求項１４，１５または１６において、少なくとも前記解読鍵識別子は暗号化せずに転送する情報転送方式。

【請求項１９】送信端末から受信端末に情報を暗号化し、暗号化情報をパケット化して転送する情報転送方式において、前記送信端末は２種類以上の暗号化鍵を用いて情報を暗号化し、パケットを組み立て、前記受信端末に転送することを特徴とする情報転送方式。

【請求項２０】請求項１９において、前記送信端末は使用する前記暗号化鍵を一意に示す前記暗号化鍵識別子を

決定する手段を具備し、前記暗号化情報を転送する毎に前記暗号化鍵識別子を前記暗号化情報と共に転送し、前記受信端末は受信した情報の中の前記暗号化鍵識別子から前記解読鍵を決定する手段を具備し、前記解読鍵を用いて前記受信情報を解読する情報転送方式。

【請求項２１】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は送信端末アドレスと受信端末アドレスのいずれか一方、あるいは両方から暗号化鍵を決定し、前記受信端末は受信した情報の中の前記送信端末アドレスと前記受信端末アドレスのいずれか一方、あるいは両方から解読鍵を決定することを特徴とする情報転送方式。

【請求項２２】請求項２１において、前記暗号化鍵を決定する手段として、一つあるいは複数の前記送信端末アドレスと一つの前記暗号化鍵を関連付けて記憶する手段を具備し、解読鍵を決定する手段として、一つあるいは複数の前記送信端末アドレスと一つの前記解読鍵を関連付けて記憶する手段を具備する情報転送方式。

【請求項２３】請求項２１において、前記暗号化鍵を決定する手段として、一つあるいは複数の前記受信端末アドレスと一つの前記暗号化鍵を関連付けて記憶する手段を具備し、前記解読鍵を決定する手段として、一つあるいは複数の前記受信端末アドレスと一つの前記解読鍵を関連付けて記憶する手段を具備する情報転送方式。

【請求項２４】請求項２１において、前記暗号化鍵を決定する手段として、一つあるいは複数の前記送信端末アドレスと前記受信端末アドレスの組み合わせと一つの前記暗号化鍵を関連付けて記憶する手段を具備し、前記解読鍵を決定する手段として、一つあるいは複数の前記送信端末アドレスと前記受信端末アドレスの組み合わせと一つの前記解読鍵を関連付けて記憶する手段を具備する情報転送方式。

【請求項２５】請求項２１，２２，２３または２４において、前記送信端末は、少なくとも前記送信端末アドレスと前記受信端末アドレスのいずれか一方、あるいは両方を暗号化せずに、前記転送情報と共に転送する情報転送方式。

【請求項２６】請求項２１，２２，２３または２４において、前記送信端末は、前記送信端末アドレスと前記受信端末アドレスのいずれか一方、あるいは両方を共通鍵を用いて暗号化して、前記転送情報と共に転送する情報転送方式。

【請求項２７】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は、前記送信端末から前記受信端末への転送経路を示すルート情報から暗号化鍵を決定し、前記受信端末は受信した情報の中の前記ルート情報から解読鍵を決定することを特徴とする情報転送方式。

【請求項２８】請求項２７において、前記暗号化鍵を決定する手段として、一つあるいは複数のルート情報と一つの前記暗号化鍵を関連付けて記憶する手段を具備し、解読鍵を決定する手段として、一つあるいは複数の前記ルート情報と一つの前記解読鍵を関連付けて記憶する手段を具備する情報転送方式。

【請求項２９】請求項２７または２８において、前記送信端末は少なくとも前記ルート情報を暗号化せずに前記転送情報と共に転送する情報転送方式。

【請求項３０】請求項２７または２８において、前記送信端末は少なくとも前記ルート情報を前記共通鍵を用いて暗号化して前記転送情報と共に転送する情報転送方式。

【請求項３１】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、フロッピーディスクからのローディング，リード・オンリー・メモリからのローディング，通信端末あるいは制御端末からのコマンド入力の内、少なくとも一つの手段により暗号化鍵を設定することを特徴とする情報伝送方式。

【請求項３２】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、フロッピーディスクからのローディング，リードオンリーメモリからのローディング，通信端末あるいは制御端末からのコマンド入力の内、任意の複数の設定手段を有し、更に任意の設定手段を選択することを特徴とする情報転送方式。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、送信側通信端末（以下、送信端末と称す）から受信側通信端末（以下、受信端末と称す）に情報を暗号化して転送する情報転送方式に係り、特に、転送情報の送信先によって異なる暗号化アルゴリズム（以下、暗号化鍵と称す）を用いて情報を暗号化し転送する情報転送方式に関する。

【０００２】

【従来の技術】暗号を用いた従来の秘匿通信方式として、特開平3－262227 号公報に開示の技術がある。

【０００３】上記従来技術では、二つの通信局間で秘匿通信を行うために、双方の通信局に多数の暗証コードおよび暗号コード（暗号化鍵）を同じアドレスに記憶した暗証／暗号メモリを具備する。送信局は受信局に対して暗証／暗号メモリのアドレスを指定した応答要求信号を送信し、受信局は指定されたアドレスに記憶された暗証コードを読み出して、暗証コードを応答信号にのせて送信局に返信する。送信局は応答信号の暗証コードが正しいことを確認した後に、同アドレスの暗号コードを読み出し、暗号コードを用いて情報を暗号化した後に受信局に送信する。一方、受信局はアドレスの暗号コードを読み出し、暗号コードを用いて受信情報の解読を行う。

【０００４】

【発明が解決しようとする課題】上記従来技術をローカルエリアネットワーク（以下、ＬＡＮと称す）の様なコネクションレス通信（以下、ＣＬ通信と称す）に適用す

5

る場合には次のような問題点が生じる。

【０００５】先ず、ＣＬ通信には明確な通信の開始が無いので、秘匿通信に先立って暗号コードを転送することが出来ないという問題点がある。これに対して単一の暗号コードを使用するという方式が考えられるが、単一暗号コードを使用した場合は暗号コードを第三者が獲得しネットワーク内の情報を無断で入手する危険性が高くなるので好ましくない。

【０００６】ネットワークのセキュリティを向上させるには複数の暗号コードを用いれば良いが、ＣＬ通信では前述の様に通信に先立って暗号コードを通知することが出来ないので、次のような新たな問題点が発生する。すなわち、ＣＬ通信ではネットワーク内の各端末が受信するのは必ずしも自分宛の情報とは限らない。即ち、各端末はネットワーク上の転送情報を監視し、転送情報（バケット）に含まれるルート情報に基づきバケットが自分宛か否かを判断しバケットの取捨選択を行う。ここで、ネットワーク内で複数の異なる暗号化コードを用いて複数の異なるルート情報を暗号化した場合、異なるルート情報から同一の暗号化ルート情報が生成することが考えられる。即ち、このような場合には送受信端末間で暗号コードを一致させておかないと、本来受信しない情報を誤って受信してしまうことになる。

【０００７】従来技術の類似技術として、ＣＬ通信の任意の時点（例えば、始業時間）に暗号コードを通知するようにして、更に、異なるルート情報からは異なる暗号化ルート情報しか生成しないようにしても次のような問題点が生じる。すなわち、前述の様に、ＣＬ通信ではネットワーク上のバケットの取捨選択によりバケットを受信するか否かを決定するので、受信端末はバケット受信毎に全ての暗号コードを用いてバケットを解読しなくてはならない。これはネットワークのスループットの低下の原因になるばかりでなく、ハード量の増加の原因にもなる。

【０００８】本発明の目的は、送受信端末間の情報授受の機密性を維持するために複数の暗号化コード（暗号化鍵）を用いる情報転送方式において、暗号化情報の誤受信とこれに伴うスループットの低下、およびハード量の増加を防ぐ情報転送方式を提供することにある。

【０００９】

【課題を解決するための手段】前記課題を解決する第一の手段として、暗号化鍵を暗号化情報と共に転送する手段を送信端末に設け、受信した情報の中の暗号化鍵から解読鍵を決定する手段を受信端末に設ける。

【００１０】前記課題を解決する第二の手段として、暗号化鍵に対応する解読鍵を暗号化情報と共に転送する手段を送信端末に設け、受信した情報の中の解読鍵を読み出す手段を受信端末に設ける。

【００１１】前記課題を解決する第三の手段として、使用する暗号化鍵を一意に示す暗号化鍵識別子を決定する

6

手段と、前記暗号化鍵識別子を暗号化情報と共に転送する手段を送信端末に設け、受信した情報の中の暗号化鍵識別子から解読鍵を決定する手段を受信端末に設ける。

【００１２】前記課題を解決する第四の手段として、使用する暗号化鍵に対応する解読鍵を一意に示す解読鍵識別子を決定する手段と、前記解読鍵識別子を暗号化情報と共に転送する手段を送信端末に設け、受信した情報の中の解読鍵識別子から解読鍵を決定する手段を受信端末に設ける。

【００１３】前記課題を解決する第五の手段として、送信端末アドレスと受信端末アドレスのいずれか一方、あるいは両方から暗号化鍵を決定する手段を送信端末に設け、受信した情報の中の送信端末アドレスと受信端末アドレスのいずれか一方、あるいは両方から解読鍵を決定する手段を受信端末に設ける。

【００１４】前記課題を解決する第六の手段として、ルート情報から暗号化鍵を決定する手段を送信端末に設け、受信した情報の中のルート情報から解読鍵を決定する手段を受信端末に設ける。

【００１５】

【作用】第一の解決手段を用いた情報転送方式では、暗号化鍵を暗号化情報と共に転送する手段により、暗号化情報に付随して受信端末に暗号化鍵を通知することが可能になる。更に、受信した情報の中の暗号化鍵から解読鍵を決定する手段により、受信端末は送信端末が使用した暗号化鍵に対応する解読鍵を決定することが出来る。本情報転送方式では暗号化情報と暗号化鍵が対になって転送され、更に暗号化鍵から解読鍵を決定することが出来るので、複数の暗号化鍵を用いる場合でも暗号化情報を正確に解読することが可能になる。

【００１６】第二の解決手段を用いた情報転送方式では、暗号化鍵に対応する解読鍵を暗号化情報と共に転送する手段により、暗号化情報に付随して受信端末に解読鍵を通知することが可能になる。更に、受信した情報の中の解読鍵を読み出す手段により、受信端末は送信端末が使用した暗号化鍵に対応する解読鍵を決定することが出来る。本情報転送方式では暗号化情報と対応する解読鍵が対になって転送されるので、複数の暗号化鍵を用いる場合でも暗号化情報を正確に解読することが可能になる。

【００１７】第三の解決手段を用いた情報転送方式では、使用する暗号化鍵を一意に示す暗号化鍵識別子を暗号化情報と共に転送する手段により、受信端末に暗号化鍵識別子を通知することが可能になる。更に、暗号化鍵識別子から解読鍵を決定する手段により、暗号化鍵識別子に対して一組の暗号化鍵／解読鍵が定まる。本情報転送方式では暗号化情報と暗号化鍵識別子が対になって転送されるので、複数の暗号化鍵を用いる場合でも暗号化情報を正確に解読することが可能になる。

【００１８】第四の解決手段を用いた情報転送方式で

は、使用する暗号化鍵に対応する解読鍵を一意に示す解読鍵識別子を暗号化情報と共に転送する手段により、受信端末に解読鍵識別子を通知することが可能になる。更に、解読鍵識別子から解読鍵を決定する手段により、解読鍵識別子に対して一組の暗号化鍵／解読鍵が定まる。本情報転送方式では暗号化情報と解読鍵識別子が対になって転送されるので、複数の暗号化鍵を用いる場合でも暗号化情報を正確に解読することが可能になる。

【００１９】第五の解決手段を用いた情報転送方式では、送信端末アドレスと受信端末アドレスのいずれか一方、あるいは両方から暗号化鍵を決定する手段と、受信した情報の中の送信端末アドレスと受信端末アドレスのいずれか一方、あるいは両方から解読鍵を決定する手段により、送信端末アドレスと受信端末アドレスのいずれか一方、あるいは両方のアドレスに対して一組の暗号化鍵／解読鍵が定まる。本情報転送方式では送信端末アドレスと受信端末アドレスを暗号化情報と共に転送するので、複数の暗号化鍵を用いる場合でも暗号化情報を正確に解読することが出来る。

【００２０】第六の解決手段を用いた情報転送方式では、ルート情報から暗号化鍵を決定する手段と、受信した情報の中のルート情報から解読鍵を決定する手段により、ルート情報に対して一組の暗号化鍵／解読鍵が定まる。本情報転送方式ではルート情報を暗号化情報と共に転送するので、複数の暗号化鍵を用いる場合でも暗号化情報を正確に解読することが出来る。

【００２１】

【実施例】図２は本発明を用いたＬＡＮ接続ボード１４０（以下、ＬＡＮインタフェースと称す）を装着したワークステーション（以下、ＷＳと称す）本体１００のブロック図である。

【００２２】図２において、ユーザＩ／Ｏインタフェース１１０，ＣＰＵ１２０，メモリ１３０，ＬＡＮインタフェース１４０，ＦＤ制御部１５０が内部バス１６０で接続されている。ユーザＩ／Ｏインタフェース１１０はＷＳ本体１００と入力装置（キーボード）および出力装置（ディスプレイ）のインタフェースであり、キーボードからの入力信号の内部バス１６０への転送、内部バス１６０からの信号のディスプレイへの出力等の機能を持つ。尚、本実施例では入力装置をキーボード、出力装置をディスプレイとしたが本構成は本発明を限定するものではない。

【００２３】ＣＰＵ１２０はキーボードから入力する情報、およびＬＡＮインタフェース１４０を介して入力する他端末等からの情報の処理と各機能ブロックの制御を行うブロックである。メモリ１３０は前述の各種情報を格納する機能ブロックであり、ＣＰＵ１２０の処理待ち、ディスプレイへの出力待ち等の場合に当該情報を格納する。ＬＡＮインタフェース１４０はＷＳをネットワーク（ＬＡＮ）に接続するための機能を有するブロックであり、内部バス１６０の伝送フォーマットとＬＡＮの伝送フォーマットの変換を行うと共に、ＭＡＣ(Media Access Control)層の終端、転送情報の暗号化を行う。ＦＤ制御部１５０はＣＰＵ１２０の指示に従って、フロッピーディスク（以下ＦＤ）からのローディング，ＦＤへのセーブ等の機能を持つ。内部バス１６０はＷＳが処理するデータを転送するデータバスと、各機能ブロックを制御するための制御情報を転送する制御情報バスからなる。

【００２４】図３はＬＡＮインタフェース１４０の機能ブロック図である。ＬＡＮインタフェース１４０はバスインタフェース１７０，ＬＡＮ制御部１８０，ＲＯＭ１９０，暗号化部２００，伝送部２１０から構成される。

【００２５】バスインタフェース１７０は内部バス１６０からの情報ブロックの切り出し、情報ブロックのＬＡＮ制御部１８０への転送、更に、ＬＡＮ制御部１８０から転送された情報ブロックのバッファリング、情報ブロックの内部バスへの乗せ換えを行う。ＬＡＮ制御部１８０はバケットの生成／分解，バケットヘッダの付加／削除等のＭＡＣレイヤ機能を実現するブロックである。バケットヘッダには送信端末アドレス（送信元アドレス）と受信端末アドレス（宛先アドレス）が含まれる。送信元アドレスにはＲＯＭ１９０に登録されているＭＡＣアドレスが書き込まれる。ＲＯＭ１９０に登録されているＭＡＣアドレスは、ＷＳだけに割り当てられたアドレスである。一方、宛先アドレスにはバケットの送信先のＷＳに割り当てられたＭＡＣアドレスが書き込まれる。これらの宛先ＷＳのＭＡＣアドレスはデータベースとしてＬＡＮ制御部１８０内のメモリに記憶されている。暗号化部２００はＬＡＮ制御部１８０からの情報の暗号化を行うと共に、ＬＡＮから受信した暗号化情報を解読しＬＡＮ制御部１８０に転送する。伝送部２１０は暗号化部２００からの情報を、接続するＬＡＮの伝送フォーマットに変換しＬＡＮに転送する。また、ＬＡＮから転送される情報を自ＷＳ内のフォーマットに変換する。

【００２６】次に図１を用いて暗号化部２００を詳細に説明する。図１において、入力バケットカウント回路２１１はＬＡＮ制御部１８０から入力するバケット数をカウントし、カウント値を暗号化鍵／ＩＤ読み出し回路２１２に転送する。暗号化鍵／ＩＤ読み出し回路２１２はカウント値に基づき、バケットの暗号化に使用する暗号化鍵と暗号化鍵を一意に示す暗号化鍵識別子（以下、暗号化鍵ＩＤと称す）をメモリ２１３より読み出す。

【００２７】図４（ａ）にメモリ２１３の構成例を示す。本実施例では０から２５５までのカウント値３０１に対して、一対一に対応するように暗号化鍵３０２が２５６種類登録されており、各暗号化鍵に１６進表示で００からＦＦまでの暗号化鍵ＩＤ３０３が登録させている。尚、異なる複数の暗号化鍵ＩＤに対して同一の暗号化鍵を対応させることも可能である。そのような場合に

は、２５６種類のカウント値と暗号化鍵ＩＤに対して２５６種類以下の暗号化鍵が登録される。更に、暗号化鍵／ＩＤ読み出し回路２１２は暗号化鍵を暗号化回路２１５に転送すると共に、暗号化鍵ＩＤを暗号化鍵ＩＤ挿入回路２１６に転送する。バッファ２１４は暗号化鍵の転送までの時間だけＬＡＮ制御部１８０から入力したバケットを格納する。暗号化鍵ＩＤ挿入回路２１６はバケットの所定の位置に、暗号化鍵／ＩＤ読み出し回路２１２より転送された暗号化鍵ＩＤを挿入する。

【００２８】図５に本実施例における暗号化鍵ＩＤ５０４の挿入位置を示す。バケット500はバケットヘッダと情報領域５０１から構成される。バケットヘッダ内には宛先アドレス５０２と送信元アドレス５０３が書き込まれている。暗号化鍵ID504 はユーザ情報５０５とバケットヘッダの間に挿入する。ＭＡＣ層では、暗号化鍵ＩＤ５０４とユーザ情報５０５を情報領域５０１として取扱うので、暗号化鍵ＩＤ５０４の挿入はＭＡＣ層プロトコルには影響を及ぼさない。

【００２９】一方、暗号化回路２１５はバッファ２１４より入力するバケットを暗号化し、暗号化鍵ＩＤ挿入回路２１６に転送する。本実施例では、暗号化鍵ＩＤはネットワーク内の全ての通信機器が解読可能な暗号化鍵（以下、共通暗号化鍵と称す）を用いて暗号化し、その他の部分はメモリ２１３より読み出した個別の暗号化鍵を用いて暗号化する。

【００３０】次に、ＬＡＮから暗号化情報を受信したときの処理について説明する。暗号化鍵ＩＤ分離回路２１７は受信暗号化バケットから暗号化鍵ＩＤの区間を切り出し、解読鍵読み出し回路２１８に転送する。暗号化鍵ＩＤ以外の部分はそのままバッファ２２０に格納される。解読鍵読み出し回路２１８は暗号化鍵ＩＤに基づき、メモリ２１９より解読鍵を読み出す。暗号化鍵ＩＤは共通暗号化鍵で暗号化されているので、全ての受信端末は暗号化鍵ＩＤを解読することができる。尚、本実施例では暗号化鍵ＩＤの暗号化に共通暗号化鍵を用いているので平文の暗号化鍵ＩＤと暗号化した暗号化鍵ＩＤは一対一に対応するので、受信したバケットの暗号化鍵ＩＤを解読せずに用いて解読鍵を選択することも可能である。また、暗号化鍵ＩＤを暗号化せずにその他の暗号化情報と共に転送することも可能であり、その場合は暗号化鍵ＩＤ分離回路２１７が切り出した暗号化鍵ＩＤをそのまま用いて解読鍵を選択する。

【００３１】図４（ｂ）にメモリ２１９の構成例を示す。本実施例では１６進表示で００からＦＦまでの暗号化鍵ＩＤ４０１に対して、一対一に対応するように解読鍵402が２５６種類登録されている。尚、メモリ２１３と同様に異なる複数の暗号化鍵ＩＤに対して同一の解読鍵を対応させることも可能である。そのような場合には２５６種類の暗号化鍵ＩＤに対して２５６種類以下の解読鍵が登録される。解読鍵読み出し回路２１８は暗号化鍵ＩＤで一意に定まる解読鍵を読み出し、解読回路２２１に転送する。解読回路２２１は、バッファ２２０より入力するバケットを解読鍵を用いて解読し、ＬＡＮ制御部１８０に転送する。

【００３２】次に本実施例におけるカウント値／暗号化鍵／暗号化鍵ＩＤ／解読鍵の設定方法について説明する。本実施例ではシステム構築時に、フロッピーディスク(FD)より設定データをロードする。カウント値／暗号化鍵／暗号化鍵ＩＤを登録するメモリ２１３への設定データの書き込み制御はメモリ書込制御２２２が行う。一方、暗号化鍵ＩＤ／解読鍵を登録するメモリ２１９への設定データの書き込み制御はメモリ書込制御２２３が行う。尚、設定データの変更が生じた場合には、ネットワーク内の通信端末あるいは制御端末からのコマンド入力によりメモリ内の登録内容の書き換えを行う。この場合には、ＷＳ本体１００内のＣＰＵ１２０で処理された設定データが内部バス１６０を介してメモリ書込制御２２２およびメモリ書込制御２２３に転送される。書込制御２２２および２２３はＣＰＵ１２０の指示に基づき、メモリ２１３およびメモリ２１９の登録内容の書き換えを行う。

【００３３】次に図６，図７を用いて第二の実施例について説明する。本実施例ではＬＡＮ制御部１８０から入力するバケットの宛先アドレスに基づいて使用する暗号化鍵を決定する。尚、本実施例は第一の実施例と暗号化部２００の動作のみが異なるので、暗号化部２００のみ説明する。

【００３４】図６において、宛先アドレス読み出し回路２２４はＬＡＮ制御部１８０から入力するバケットの宛先アドレスを読み出し、暗号化鍵読み出し回路２２５に転送する。暗号化鍵読み出し回路２２５は宛先アドレスに基づき、使用する暗号化鍵をメモリ２１３より読み出す。

【００３５】図７（ａ）に本実施例におけるメモリ２１３の構成例を示す。メモリ２１３では２５６種類の送信バケット宛先アドレス３０４（ＤＡ＃０～ＤＡ＃２５５）に対して、一対一に対応するように暗号化鍵３０２が２５６種類登録されている。宛先アドレスには各端末への個別通信用のアドレスと複数の端末に共通に付与されているグループ通信用のアドレスと、全ての端末に共通に付与されている一斉同報通信用のアドレスがある。尚、異なる複数の宛先アドレスに対して同一の暗号化鍵を対応させることも可能である。そのような場合には２５６種類の宛先アドレスに対して２５６種類以下の暗号化鍵が登録される。更に、宛先アドレスと送信元アドレスの組み合わせに対して、一対一に対応するように暗号化鍵を登録することも可能である。更に、暗号化鍵読み出し回路２２５は暗号化鍵を暗号化回路２１５に転送する。バッファ２１４は暗号化鍵の転送までの時間だけＬＡＮ制御部１８０から入力したバケットを格納する。暗

号化回路２１５はバッファ２１４より入力するパケットを暗号化し、伝送部２１０に転送する。本実施例では、宛先アドレスと送信元アドレスは共通暗号化鍵を用いて暗号化し、その他の部分はメモリ２１３より読み出した暗号化鍵を用いて暗号化する。

【００３６】本実施例では、第一の実施例における暗号化鍵ＩＤのような特有のパラメータを使用しないので、暗号化部２００と伝送部２１０の間で授受するパケットフォーマットはＬＡＮ制御部がサポートするＭＡＣ層プロトコルのパケットフォーマットと一致する。

【００３７】次に、ＬＡＮから暗号化情報（パケット）を受信したときの処理について説明する。宛先アドレス分離回路２２６は暗号化パケットから宛先アドレスの区間を複写し、解読鍵読み出し回路２１８に転送する。解読鍵読み出し回路２１８は宛先アドレスに基づき、メモリ２１９より解読鍵を読み出す。宛先アドレスは共通暗号化鍵で暗号化されているので、全ての受信端末は宛先アドレスを解読することができる。尚、本実施例では宛先アドレスの暗号化に共通暗号化鍵を用いていることから平文の宛先アドレスと暗号化した宛先アドレスは一対一に対応するので、受信したパケットの宛先アドレスを解読せずに用いて解読鍵を選択することも可能である。また、宛先アドレスを暗号化せずにその他の暗号化情報と共に転送することも可能であり、その場合は宛先アドレス分離回路２２６が複写した宛先アドレスをそのまま用いて解読鍵を選択する。

【００３８】図７（ｂ）にメモリ２１９の構成例を示す。本実施例では（Ｎ＋２）種類の受信パケットの宛先アドレス４０３に対して（Ｎ＋２）種類の解読鍵４０２が一対一に対応するように登録されている。具体的には、自ＷＳが個別通信の受信端末となる場合の自アドレス１種類、自ＷＳを含むグループに対するグループ通信を行う場合のグループアドレスＮ種類、全ての端末に対する同報通信を行う場合の一斉同報アドレス１種類の計（Ｎ＋２）種類のアドレスに対して、一対一に対応するように（Ｎ＋２）種類の解読鍵４０２が登録されている。尚、異なる複数の受信パケット宛先アドレスに対して同一の解読鍵を対応させることも可能である。そのような場合には（Ｎ＋２）種類の宛先アドレスに対して（Ｎ＋２）種類以下の解読鍵が登録される。更には、宛先アドレスと発信元アドレスの組み合わせに対して、一対一に対応するように解読鍵を登録することも可能である。解読鍵読み出し回路２１８は宛先アドレスで一意に定まる解読鍵を読み出し、解読回路２２１に転送する。解読回路２２１はバッファ２２０より入力するパケットを解読鍵を用いて解読し、ＬＡＮ制御部１８０に転送する。

【００３９】次に本実施例における送信パケット宛先アドレス／暗号化鍵および受信パケット宛先アドレス／解読鍵の設定方法について説明する。本実施例ではシステム構築時に、ＦＤより設定データをロードする。送信パケット宛先アドレス／暗号化鍵を登録するメモリ２１３への設定データの書き込み制御はメモリ書込制御２２２が行う。一方、受信パケット宛先アドレス／解読鍵を登録するメモリ２１９への設定データの書き込み制御はメモリ＃２書込制御２２３が行う。尚、設定データの変更が生じた場合には、ネットワーク内の通信端末あるいは制御端末からのコマンド入力によりメモリ内の登録内容の書き換えを行う。この場合には、ＷＳ本体１００内のＣＰＵ１２０で処理された設定データが内部バス１６０を介してメモリ書込制御２２２およびメモリ書込制御２２３に転送される。書込制御２２２，２２３はＣＰＵ１２０の指示に従い、メモリ２１３，メモリ２１９の登録内容の書き換えを行う。

【００４０】次に図８，図９を用いて第三の実施例について説明する。本実施例ではＬＡＮ制御部１８０から入力するパケットのルート情報に基づいて使用する暗号化鍵を決定する。尚、本実施例も前述の第一の実施例と暗号化部２００の動作のみが異なるので、暗号化部２００のみ説明する。

【００４１】図８において、ルート情報読み出し回路２２７はＬＡＮ制御部１８０から入力するパケットのルート情報を読み出し、暗号化鍵読み出し回路２２５に転送する。暗号化鍵読み出し回路２２５はルート情報に基づき、使用する暗号化鍵をメモリ２１３より読み出す。

【００４２】図９（ａ）に本実施例におけるメモリ２１３の構成例を示す。メモリ２１３では２５６種類の送信パケットルート情報３０５（ＶＣＮ＃０～ＶＣＮ＃２５５）に対して、一対一に対応するように暗号化鍵３０２が２５６種類登録されている。尚、ルート情報の設定方法は任意であり本発明を制限するものではない。暗号化鍵読み出し回路２２５は暗号化鍵を暗号化回路２１５に転送する。バッファ２１４は前記暗号化鍵の転送までの時間だけＬＡＮ制御部１８０から入力したパケットを格納する。暗号化回路２１５はバッファ２１４より入力するパケットを暗号化し、伝送部２１０に転送する。本実施例では、ルート情報は共通暗号化鍵を用いて暗号化し、その他の部分はメモリ２１３より読み出した暗号化鍵を用いて暗号化する。

【００４３】本実施例でも第一の実施例における暗号化鍵ＩＤのような特有のパラメータを使用しないので、暗号化部２００と伝送部２１０の間で授受するパケットフォーマットはＬＡＮ制御部がサポートするＭＡＣ層プロトコルのパケットフォーマットと完全に一致する。

【００４４】次に、ＬＡＮから暗号化情報（パケット）を受信したときの処理について説明する。ルート情報分離回路２２８は暗号化パケットからルート情報の区間を複写し、解読鍵読み出し回路２１８に転送する。解読鍵読み出し回路２１８はルート情報に基づき、メモリ２１９より解読鍵を読み出す。ルート情報は共通暗号化鍵で

暗号化されているので、全ての受信端末はルート情報を解読することができる。尚、本実施例ではルート情報の暗号化に共通暗号化鍵を用いているので平文のルート情報と暗号化したルート情報は一対一に対応するので、受信したパケットのルート情報を解読せずに用いて解読鍵を選択することも可能である。また、ルート情報を暗号化せずにその他の暗号化情報と共に転送することも可能であり、その場合にはルート情報分離回路２２８が複写したルート情報をそのまま用いて解読鍵を選択する。

【００４５】図９（ｂ）にメモリ２１９の構成例を示す。本実施例では受信パケットのルート情報４０４に対して、一対一に対応するように２５６種類の解読鍵４０２が登録されている。尚、異なる複数のルート情報に対して同一の解読鍵を対応させることも可能である。そのような場合には２５６種類のルート情報に対して２５６種類以下の解読鍵が登録される。解読鍵読み出し回路２１８はルート情報で一意に定まる解読鍵を読み出し、解読回路２２１に転送する。解読回路２２１はバッファ２２０より入力するパケットを解読鍵を用いて解読し、ＬＡＮ制御部１８０に転送する。

【００４６】次に本実施例における送信パケットルート情報／暗号化鍵および受信パケットルート情報／解読鍵の設定方法について説明する。本実施例ではシステム構築時に、ＦＤより設定データをロードする。送信パケットルート情報／暗号化鍵を登録するメモリ２１３への設定データの書き込み制御はメモリ２１３の書込制御２２２が行う。一方、受信パケットルート情報／解読鍵を登録するメモリ２１９への設定データの書き込み制御はメモリ２１９の書込制御２２３が行う。尚、設定データの変更が生じた場合には、ネットワーク内の通信端末あるいは制御端末からのコマンド入力によりメモリ内の登録内容の書き換えを行う。この場合には、ＷＳ本体１００内のＣＰＵ１２０で処理された設定データが内部バス１６０を介してメモリ＃１書込制御２２２およびメモリ＃２書込制御２２３に転送される。書込制御２２２および２２３はＣＰＵ１２０の指示に基づき、メモリ２１３およびメモリ２１９の登録内容の書き換えを行う。

【００４７】次に図１０，図１１を用いて第四の実施例について説明する。本実施例ではパケットを送信する通信端末のＭＡＣアドレスに基づいて使用する暗号化鍵を決定する。従って、物理的に一つの通信端末が複数のＭＡＣアドレスを有する場合には一端末が複数の暗号化鍵を有することになり、複数の通信端末が一つのＭＡＣアドレスを共有する場合には複数の端末が一つの暗号化鍵を共有することになる。尚、本実施例も前述の第一の実施例と暗号化部２００の動作のみが異なるので、暗号化部２００のみ説明する。

【００４８】図１０において、送信元アドレス読み出し回路２２９はＬＡＮ制御部１８０から入力するパケットの送信元アドレスを読み出し、暗号化鍵読み出し回路２２５に転送する。暗号化鍵読み出し回路２２５は前記送信元アドレスに基づき、使用する暗号化鍵をメモリ２１３より読み出す。

【００４９】図１１（ａ）に本実施例におけるメモリ２１３の構成例を示す。本実施例では１種類の送信パケット送信元アドレス３０６に対して一種類の暗号化鍵３０２が登録されている。暗号化鍵読み出し回路２２５は暗号化鍵を暗号化回路２１５に転送する。バッファ２１４は暗号化鍵の転送までの時間だけＬＡＮ制御部１８０から入力したパケットを格納する。暗号化回路２１５はバッファ２１４より入力するパケットを暗号化し、伝送部２１０に転送する。本実施例では、宛先アドレスと送信元アドレスは共通暗号化鍵を用いて暗号化し、その他の部分はメモリ２１３より読み出した暗号化鍵を用いて暗号化する。

【００５０】本実施例でも第一の実施例における暗号化鍵ＩＤのような特有のパラメータを使用しないので、暗号化部２００と伝送部２１０の間で授受するパケットフォーマットはＬＡＮ制御部がサポートするＭＡＣ層プロトコルのパケットフォーマットと一致する。

【００５１】次に、ＬＡＮから暗号化情報（パケット）を受信したときの処理について説明する。送信元アドレス分離回路２３０は暗号化パケットから送信元アドレスの区間を複写し、解読鍵読み出し回路２１８に転送する。解読鍵読み出し回路２１８は送信元アドレスに基づき、メモリ２１９より解読鍵を読み出す。送信元アドレスは共通暗号化鍵で暗号化されているので、全ての受信端末は送信元アドレスを解読することができる。尚、本実施例では送信元アドレスの暗号化に共通暗号化鍵を用いていることから平文の送信元アドレスと暗号化した送信元アドレスは一対一に対応するので、受信したパケットの送信元アドレスを解読せずに用いて解読鍵を選択することも可能である。また、送信元アドレスを暗号化せずにその他の暗号化情報と共に転送することも可能であり、その場合には送信元アドレス分離回路２３０が複写した送信元アドレスをそのまま用いて解読鍵を選択する。

【００５２】図１１（ｂ）にメモリ２１９の構成例を示す。本実施例では２５６種類の受信パケットの送信元アドレス４０５に対して２５６種類の解読鍵４０２が一対一に対応するように登録されている。尚、異なる複数の受信パケット送信元アドレスに対して同一の解読鍵を対応させることも可能である。そのような場合には２５６種類の宛先アドレスに対して２５６種類以下の解読鍵が登録される。解読鍵読み出し回路２１８は送信元アドレスで一意に定まる解読鍵を読み出し、解読回路２２１に転送する。解読回路２２１はバッファ２２０より入力するパケットを解読鍵を用いて解読し、ＬＡＮ制御部１８０に転送する。

【００５３】次に本実施例における送信パケット送信元

アドレス／暗号化鍵および受信パケット送信元アドレス／解読鍵の設定方法について説明する。本実施例ではシステム構築時に、ＦＤより設定データをロードする。送信パケット送信元アドレス／暗号化鍵を登録するメモリ２１３への設定データの書き込み制御はメモリ２１３書込制御２２２が行う。一方、受信パケット送信元アドレス／解読鍵を登録するメモリ２１９への設定データの書き込み制御はメモリ２１９の書込制御２２３が行う。尚、設定データの変更が生じた場合には、ネットワーク内の通信端末あるいは制御端末からのコマンド入力によりメモリ内の登録内容の書き換えを行う。この場合には、ＷＳ本体１００内のＣＰＵ１２０で処理された設定データが内部バス１６０を介してメモリ２１３の書込制御２２２およびメモリ２１９の書込制御２２３に転送される。書込制御２２２および２２３はＣＰＵ１２０の指示に基づき、メモリ２１３およびメモリ２１９の登録内容の書き換えを行う。

【００５４】次に図１２，図１３および１４を用いて第五の実施例について説明する。第一の実施例が暗号化鍵ＩＤを暗号化情報と共に転送するのに対して、本実施例は暗号化鍵を暗号化情報と共に転送する。尚、本実施例も第一の実施例と暗号化部２００の動作のみが異なるので、暗号化部２００のみ説明する。

【００５５】図１２において、入力パケットカウント回路２１１はＬＡＮ制御部１８０から入力するパケット数をカウントし、カウント値を暗号化鍵読み出し回路２３１に転送する。暗号化鍵読み出し回路２３１はカウント値に基づき、パケットの暗号化に使用する暗号化鍵をメモリ２１３より読み出す。

【００５６】図１３（ａ）にメモリ２１３の構成例を示す。本実施例では０から２５５までのカウント値３０１に対して、一対一に対応するように暗号化鍵３０２が２５６種類登録されている。尚、異なる複数のカウント値に対して同一の暗号化鍵を対応させることも可能である。そのような場合には２５６種類のカウント値に対して２５６種類以下の暗号化鍵が登録される。更に、暗号化鍵読み出し回路２３１は暗号化鍵を暗号化回路２１５と暗号化鍵挿入回路２３２に転送する。バッファ２１４は暗号化鍵の転送までの時間だけＬＡＮ制御部１８０から入力したパケットを格納する。暗号化鍵挿入回路２３２はパケットの所定の位置に、暗号化鍵読み出し回路２３１より転送された暗号化鍵を挿入する。

【００５７】図１４に本実施例における暗号化鍵５０６の挿入位置を示す。パケット５００はパケットヘッダと情報領域５０１から構成される。パケットヘッダ内には宛先アドレス５０２と送信元アドレス５０３が書き込まれている。暗号化鍵５０６はユーザ情報５０５とパケットヘッダの間に挿入する。ＭＡＣ層では、暗号化鍵５０６とユーザ情報５０５を情報領域５０１として取扱うので、暗号化鍵５０６の挿入はＭＡＣ層プロトコルには影響を及ぼさない。

【００５８】一方、暗号化回路２１５はバッファ２１４より入力するパケットを暗号化し、暗号化鍵挿入回路２３２に転送する。本実施例では、暗号化鍵はネットワーク内の全ての通信機器が解読可能な暗号化鍵（以下、共通暗号化鍵と称す）を用いて暗号化し、その他の部分はメモリ２１３より読み出した個別の暗号化鍵を用いて暗号化する。

【００５９】次に、ＬＡＮから暗号化情報を受信したときの処理について説明する。暗号化鍵分離回路２３３は受信暗号化パケットから暗号化鍵の区間を切り出し、解読鍵読み出し回路２１８に転送する。暗号化鍵以外の部分はそのままバッファ２２０に格納される。解読鍵読み出し回路２１８は暗号化鍵に基づき、メモリ２１９より解読鍵を読み出す。暗号化鍵は共通暗号化鍵で暗号化されているので、全ての受信端末は暗号化鍵を解読することができる。尚、本実施例では暗号化鍵の暗号化に共通暗号化鍵を用いていることから平文の暗号化鍵と暗号化した暗号化鍵は一対一に対応するので、受信したパケットの暗号化鍵を解読せずに用いて解読鍵を選択することも可能である。また、暗号化鍵を暗号化せずにその他の暗号化情報と共に転送することも可能であり、その場合には暗号化鍵分離回路２３３が切り出した暗号化鍵をそのまま用いて解読鍵の選択を行う。

【００６０】図１３（ｂ）にメモリ２１９の構成例を示す。本実施例では２５６種類の暗号化鍵４０６（Ｃ－Ｋｅｙ＃０～Ｃ－Ｋｅｙ＃２５５）に一対一に対応するように解読鍵４０２（Ｄ－Ｋｅｙ＃０～Ｄ－Ｋｅｙ＃２５５）が２５６種類登録されている。解読鍵読み出し回路２１８は暗号化鍵で一意に定まる解読鍵を読み出し、解読回路２２１に転送する。解読回路２２１は、バッファ２２０より入力するパケットを解読鍵を用いて解読し、ＬＡＮ制御部１８０に転送する。

【００６１】次に本実施例におけるカウント値／暗号化鍵／解読鍵の設定方法について説明する。本実施例ではシステム構築時に、フロッピーディスク（ＦＤ）より設定データをロードする。カウント値／暗号化鍵を登録するメモリ２１３への設定データの書き込み制御はメモリ＃１書込制御２２２が行う。一方、暗号化鍵／解読鍵を登録するメモリ２１９への設定データの書き込み制御はメモリ２１９の書込制御２２３が行う。尚、設定データの変更が生じた場合には、ネットワーク内の通信端末あるいは制御端末からのコマンド入力によりメモリ内の登録内容の書き換えを行う。この場合には、ＷＳ本体１００内のＣＰＵ１２０で処理された設定データが内部バス１６０を介してメモリ２１３の書込制御２２２およびメモリ219の書込制御２２３に転送される。書込制御２２２および２２３はＣＰＵ１２０の指示に基づき、メモリ２１３およびメモリ２１９の登録内容の書き換えを行う。

【００６２】次に図１５，図１６および図１７を用いて第六の実施例について説明する。第一の実施例が暗号化鍵ＩＤを暗号化情報と共に転送するのに対して、本実施例は解読鍵を暗号化情報と共に転送する。尚、本実施例も第一の実施例と暗号化部２００の動作のみが異なるので、暗号化部２００のみ説明する。

【００６３】図１５において、入力パケットカウント回路２１１はＬＡＮ制御部１８０から入力するパケット数をカウントし、カウント値を暗号化鍵／解読鍵読み出し回路２３４に転送する。暗号化鍵／解読鍵読み出し回路２３４はカウント値に基づき、パケットの暗号化に使用する暗号化鍵および解読時に使用する解読鍵をメモリ２１３より読み出す。

【００６４】図１６にメモリ２１３の構成例を示す。本実施例では０から２５５までのカウント値３０１に対して、一対一に対応するように暗号化鍵３０２と解読鍵３０７が２５６組登録されている。尚、異なる複数のカウント値に対して同一の暗号化鍵／解読鍵を対応させることも可能である。そのような場合には２５６種類のカウント値に対して２５６組以下の暗号化鍵／解読鍵が登録される。更に、暗号化鍵／解読鍵読み出し回路２３４は暗号化鍵を暗号化回路２１５に転送すると共に、解読鍵を解読鍵挿入回路２３５に転送する。バッファ２１４は暗号化鍵の転送までの時間だけＬＡＮ制御部１８０から入力したパケットを格納する。解読鍵挿入回路２３２はパケットの所定の位置に、暗号化鍵／解読鍵読み出し回路２３４より転送された解読鍵を挿入する。

【００６５】図１７に本実施例における解読鍵５０７の挿入位置を示す。パケット５００はパケットヘッダと情報領域５０１から構成される。パケットヘッダ内には宛先アドレス５０２と送信元アドレス５０３が書き込まれている。解読鍵５０７はユーザ情報５０５とパケットヘッダの間に挿入する。ＭＡＣ層では、解読鍵５０７とユーザ情報５０５を情報領域５０１として取扱うので、解読鍵５０７の挿入はＭＡＣ層プロトコルには影響を及ぼさない。

【００６６】暗号化回路２１５はバッファ２１４より入力するパケットを暗号化し、解読鍵挿入回路２３５に転送する。本実施例では、解読鍵は共通暗号化鍵を用いて暗号化し、その他の部分はメモリ２１３より読み出した個別の暗号化鍵を用いて暗号化する。

【００６７】次に、ＬＡＮから暗号化情報を受信したときの処理について説明する。解読鍵分離回路２３６は受信暗号化パケットから解読鍵の区間を切り出し、解読回路２２１に転送する。解読鍵は共通暗号化鍵で暗号化されているので、全ての受信端末は解読鍵を解読することができる。また、解読鍵を暗号化せずにその他の暗号化情報と共に転送することも可能であり、その場合には解読鍵分離回路２３６が切り出した解読鍵をそのまま用いる。解読回路２２１は解読鍵分離回路２３６より転送されるパケットを当該解読鍵を用いて解読し、ＬＡＮ制御部１８０に転送する。

【００６８】次に本実施例におけるカウント値／暗号化鍵／解読鍵の設定方法について説明する。本実施例ではシステム構築時に、フロッピーディスク（ＦＤ）より設定データをロードする。カウント値／暗号化鍵／解読鍵を登録するメモリ２１３への設定データの書き込み制御はメモリ２１３の書込制御２２２が行う。尚、設定データの変更が生じた場合には、ネットワーク内の通信端末あるいは制御端末からのコマンド入力によりメモリ内の登録内容の書き換えを行う。この場合には、ＷＳ本体１００内のＣＰＵ１２０で処理された設定データが内部バス１６０を介してメモリ２１３の書込制御２２２に転送される。書込制御２２２はCPU120の指示に基づきメモリ２１３の登録内容の書き換えを行う。

【００６９】次に図１８，図１９および２０を用いて第七の実施例について説明する。第一の実施例が暗号化鍵ＩＤを暗号化情報と共に転送するのに対して、本実施例は解読鍵識別子（以下、解読鍵ＩＤと称す）を暗号化情報と共に転送する。尚、本実施例も第一の実施例と暗号化部２００の動作のみが異なるので、暗号化部２００のみ説明する。

【００７０】図１８において、入力パケットカウント回路２１１はＬＡＮ制御部１８０から入力するパケット数をカウントし、カウント値を暗号化鍵／ＩＤ読み出し回路２１２に転送する。暗号化鍵／ＩＤ読み出し回路２１２はカウント値に基づき、パケットの暗号化に使用する暗号化鍵と暗号化鍵に対応する解読鍵を一意に示す解読鍵ＩＤをメモリ２１３より読み出す。

【００７１】図１９（ａ）にメモリ２１３の構成例を示す。本実施例では０から２５５までのカウント値３０１に対して、一対一に対応するように暗号化鍵３０２と解読鍵ＩＤ３０８が２５６組登録されている。尚、異なる複数のカウント値に対して同一の暗号化鍵／解読鍵ＩＤを対応させることも可能である。そのような場合には２５６種類のカウント値に対して２５６組以下の暗号化鍵／解読鍵ＩＤが登録される。更に、暗号化鍵／解読鍵読み出し回路２１２は暗号化鍵を暗号化回路215に転送すると共に、解読鍵ＩＤを解読鍵ＩＤ挿入回路２３７に転送する。バッファ２１４は暗号化鍵の転送までの時間だけＬＡＮ制御部１８０から入力したパケットを格納する。解読鍵ＩＤ挿入回路２３７はパケットの所定の位置に、暗号化鍵／ＩＤ読み出し回路２１２より転送された解読鍵ＩＤを挿入する。

【００７２】図２０に本実施例における解読鍵ＩＤ５０８の挿入位置を示す。パケット500はパケットヘッダと情報領域５０１から構成される。パケットヘッダ内には宛先アドレス５０２と送信元アドレス５０３が書き込まれている。解読鍵ＩＤ５０８はユーザ情報５０５とパケットヘッダの間に挿入する。ＭＡＣ層では、解読鍵ＩＤ

５０８とユーザ情報５０５を情報領域５０１として取扱うので、解読鍵ＩＤ５０８の挿入はＭＡＣ層プロトコルには影響を及ぼさない。

【００７３】暗号化回路２１５はバッファ２１４より入力するパケットを暗号化し、解読鍵ＩＤ挿入回路２３７に転送する。本実施例では、解読鍵は共通暗号化鍵を用いて暗号化し、その他の部分はメモリ２１３より読み出した個別の暗号化鍵を用いて暗号化する。

【００７４】次に、ＬＡＮから暗号化情報を受信したときの処理について説明する。解読鍵ＩＤ分離回路２３７は受信暗号化パケットから解読鍵ＩＤの区間を切り出し、解読鍵読み出し回路２１８に転送する。解読鍵ＩＤ以外の部分はそのままバッファ２２０に格納される。解読鍵読み出し回路２１８は前記解読鍵ＩＤに基づき、メモリ２１９より解読鍵を読み出す。解読鍵ＩＤは共通暗号化鍵で暗号化されているので、全ての受信端末は解読鍵ＩＤを解読することができる。尚、本実施例では解読鍵ＩＤの暗号化に共通暗号化鍵を用いていることから平文の解読鍵ＩＤと暗号化した解読鍵ＩＤは一対一に対応するので、受信したパケットの解読鍵ＩＤを解読せずに用いて解読鍵を選択することも可能である。また、解読鍵ＩＤを暗号化せずにその他の暗号化情報と共に転送することも可能であり、その場合には解読鍵ＩＤ分離回路２３８が切り出した解読鍵ＩＤをそのまま用いて解読鍵の選択を行う。

【００７５】図１９（ｂ）にメモリ２１９の構成例を示す。本実施例では２５６種類の解読鍵ＩＤ４０７に一対一に対応するように解読鍵４０２が２５６種類登録されている。解読鍵読み出し回路２１８は解読鍵ＩＤで一意に定まる解読鍵を読み出し、解読回路２２１に転送する。解読回路２２１は、バッファ２２０より入力するパケットを解読鍵を用いて解読し、ＬＡＮ制御部１８０に転送する。

【００７６】次に本実施例におけるカウント値／暗号化鍵／解読鍵ＩＤ／解読鍵の設定方法について説明する。本実施例ではシステム構築時に、フロッピーディスク(ＦＤ)より設定データをロードする。カウント値／暗号化鍵／解読鍵ＩＤを登録するメモリ２１３への設定データの書き込み制御はメモリ２１３の書込制御２２２が行う。解読鍵ＩＤ／解読鍵を登録するメモリ２１９への設定データの書き込み制御はメモリ２１９の書込制御２２３が行う。尚、設定データの変更が生じた場合には、ネットワーク内の通信端末あるいは制御端末からのコマンド入力によりメモリ内の登録内容の書き換えを行う。この場合には、ＷＳ本体１００内のCPU120で処理された設定データが内部バス１６０を介してメモリ２１３の書込制御２２２に転送される。書込制御２２２はＣＰＵ１２０の指示に基づきメモリ２１３およびメモリ２１９の登録内容の書き換えを行う。

【００７７】次に図２１，図２２を用いて第八の実施例について説明する。第七の実施例は第一の実施例とメモリ２１３，メモリ２１９の設定方法が異なる。即ち、第一の実施例ではメモリ２１３，２１９の設定はＦＤより設定データをローディングすることにより行った。本実施例では、図２１に示すようにメモリ２１３，２１９の設定データはＬＡＮインタフェース１４０内のＲＯＭ１９１から読み込む。

【００７８】図２２において、書込制御２３９はＲＯＭ１９１よりメモリ２１３への設定データ（カウント値／暗号化鍵／暗号化鍵ＩＤ）を読み込み、メモリ２１３に書き込む。書込制御２４０はＲＯＭ１９１よりメモリ２１９への設定データ（暗号化鍵ＩＤ／解読鍵）を読み込み、メモリ２１９に書き込む。

【００７９】尚、本実施例を前記第二ないし第七の実施例に適用することは容易である。第二の実施例に適用する場合には、ＲＯＭ１９１に記憶する内容を、メモリ２１３用として送信パケット宛先アドレス／暗号化鍵とし、メモリ２１９用として受信パケット宛先アドレス／解読鍵とすれば良い。第三の実施例に適用する場合には、ＲＯＭ１９１に記憶する内容を、メモリ２１３用として送信パケットルート情報／暗号化鍵とし、メモリ２１９用として受信パケットルート情報／解読鍵とすれば良い。第四の実施例に適用する場合には、ＲＯＭ１９１に記憶する内容を、メモリ２１３用として送信パケット送信元アドレス／暗号化鍵、メモリ２１９用として受信パケット送信元アドレス／解読鍵とすれば良い。第五の実施例に適用する場合には、ＲＯＭ１９１に記憶する内容を、メモリ２１３用としてカウント値／暗号化鍵、メモリ２１９用として暗号化鍵／解読鍵とすれば良い。第六の実施例に適用する場合には、ＲＯＭ１９１に記憶する内容を、メモリ２１３用としてカウント値／暗号化鍵／解読鍵とすれば良い。第七の実施例に適用する場合には、ＲＯＭ１９１に記憶する内容を、メモリ２１３用としてカウント値／暗号化鍵／解読鍵ＩＤ、メモリ２１９用として解読鍵ＩＤ／解読鍵とすれば良い。

【００８０】

【発明の効果】本発明によれば、暗号化情報と共に暗号化鍵／解読鍵を一意に示す識別情報を転送するので、複数の暗号化鍵を用いる秘匿通信においても暗号化情報を正確に解読することができる。

【００８１】識別情報として暗号化鍵あるいは解読鍵そのものを用いる場合には、任意の通信端末に対して任意の暗号化鍵を用いることが出来るので、秘匿通信の信頼性がより向上する。

【００８２】識別情報として暗号化鍵識別子あるいは解読鍵識別子を用いる場合には、任意の通信端末に対して任意の暗号化鍵を用いることが出来ることに加えて、暗号化鍵あるいは解読鍵を識別子として表現しているので、更に秘匿通信の信頼性が向上する。

【００８３】識別情報として端末アドレスあるいはルー

ト情報を用いる場合には、特別な識別子を使用することなく暗号化鍵／解読鍵を特定することが出来る。

【図面の簡単な説明】

【図１】本発明の第一の実施例における暗号化部のブロック図。

【図２】本発明の第一の実施例における通信端末（ＷＳ）本体のブロック図。

【図３】本発明の第一の実施例におけるＬＡＮインタフェースのブロック図。

【図４】本発明の第一の実施例における暗号化鍵記憶部および解読鍵記憶部の説明図。

【図５】本発明の第一の実施例におけるバケットの説明図。

【図６】本発明の第二の実施例における暗号化部のブロック図。

【図７】本発明の第二の実施例における暗号化鍵記憶部および解読鍵記憶部の説明図。

【図８】本発明の第三の実施例における暗号化部のブロック図。

【図９】本発明の第三の実施例における暗号化鍵記憶部および解読鍵記憶部の説明図。

【図１０】本発明の第四の実施例における暗号化部のブロック図。

【図１１】本発明の第四の実施例における暗号化鍵記憶部および解読鍵記憶部の説明図。

【図１２】本発明の第五の実施例における暗号化部のブロック図。

＊【図１３】本発明の第五の実施例における暗号化鍵記憶部および解読鍵記憶部の説明図。

【図１４】本発明の第五の実施例におけるバケットの説明図。

【図１５】本発明の第六の実施例における暗号化部のブロック図。

【図１６】本発明の第六の実施例における暗号化鍵および解読鍵記憶部の説明図。

【図１７】本発明の第六の実施例におけるバケットの説明図。

【図１８】本発明の第七の実施例における暗号化部のブロック図。

【図１９】本発明の第七の実施例における暗号化鍵記憶部および解読鍵記憶部の構成図。

【図２０】本発明の第七の実施例におけるバケットの説明図。

【図２１】本発明の第八の実施例におけるＬＡＮインタフェースのブロック図。

【図２２】本発明の第八の実施例における暗号化部のブロック図。

【符号の説明】

２００…暗号化部、２１１…入力バケットカウント回路、２１２…暗号化鍵／ＩＤ読み出し回路、２１３…メモリ、２１５…暗号化回路、２１６…暗号化鍵ＩＤ挿入回路、２１７…暗号化鍵ＩＤ分離回路、２１８…解読鍵読み出し回路、２１９…メモリ、２２１…解読回路、２２２…メモリ書込制御、２２３…メモリ書込制御。

【図９】

図９

(a)

305 送信パケットルート情報	303 暗号化鍵
VCN#0	C-Key#0
VCN#1	C-Key#1
⋮	⋮
VCN#254	C-Key#254
VCN#255	C-Key#255

(b)

404 受信パケットルート情報	402 解読鍵
VCN#0	D-Key#0
VCN#1	D-Key#1
⋮	⋮
VCN#254	D-Key#254
VCN#255	D-Key#255

【図１１】

図１１

(a)

306 送信パケット送信元アドレス	302 解読鍵
SA#0	C-Key#0

(b)

405 受信パケット送信元アドレス	402 解読鍵
SA#0	D-Key#0
SA#1	D-Key#1
⋮	⋮
SA#254	D-Key#254
SA#255	D-Key#255

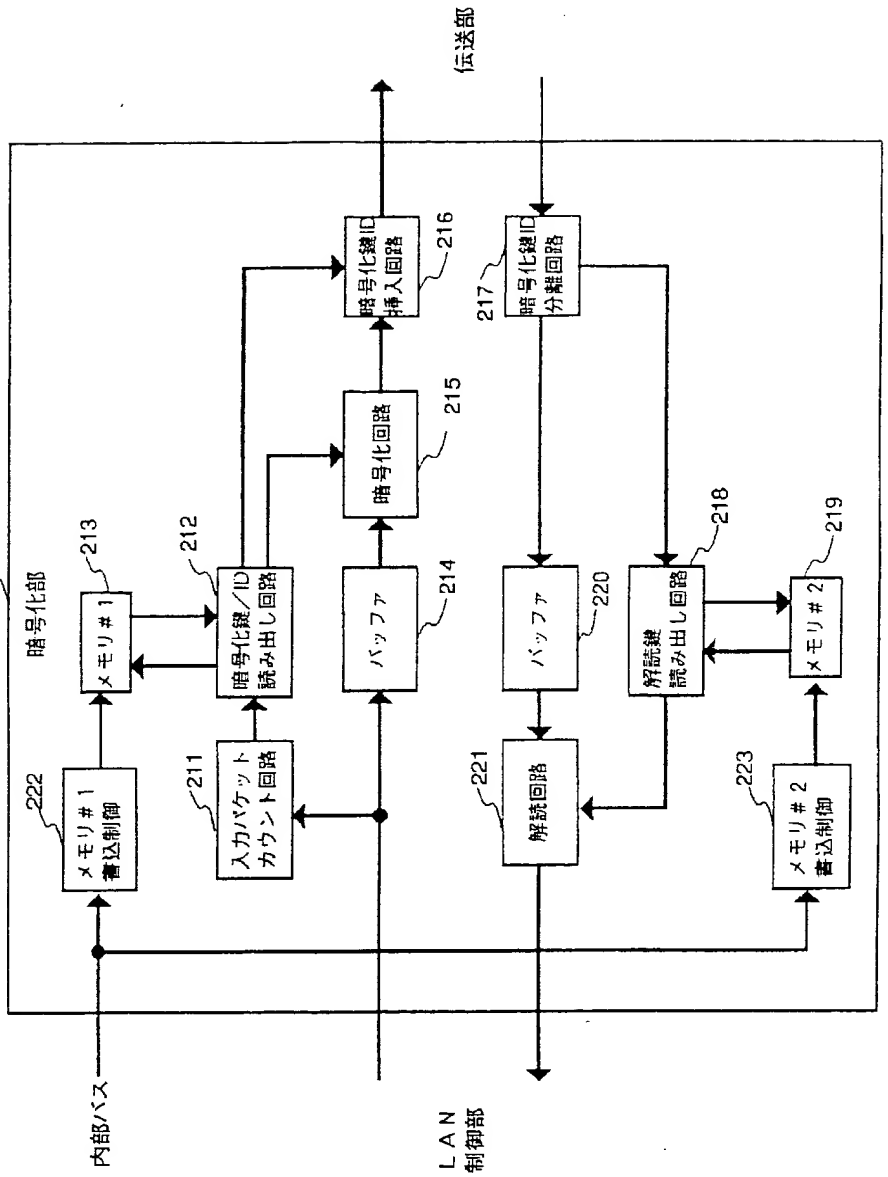
【図１６】

図１６

301 カウント値	302 暗号化鍵	307 解読鍵
0	C-Key#0	D-Key#0
1	C-Key#1	D-Key#1
⋮	⋮	⋮
254	C-Key#254	D-Key#254
255	C-Key#255	D-Key#255

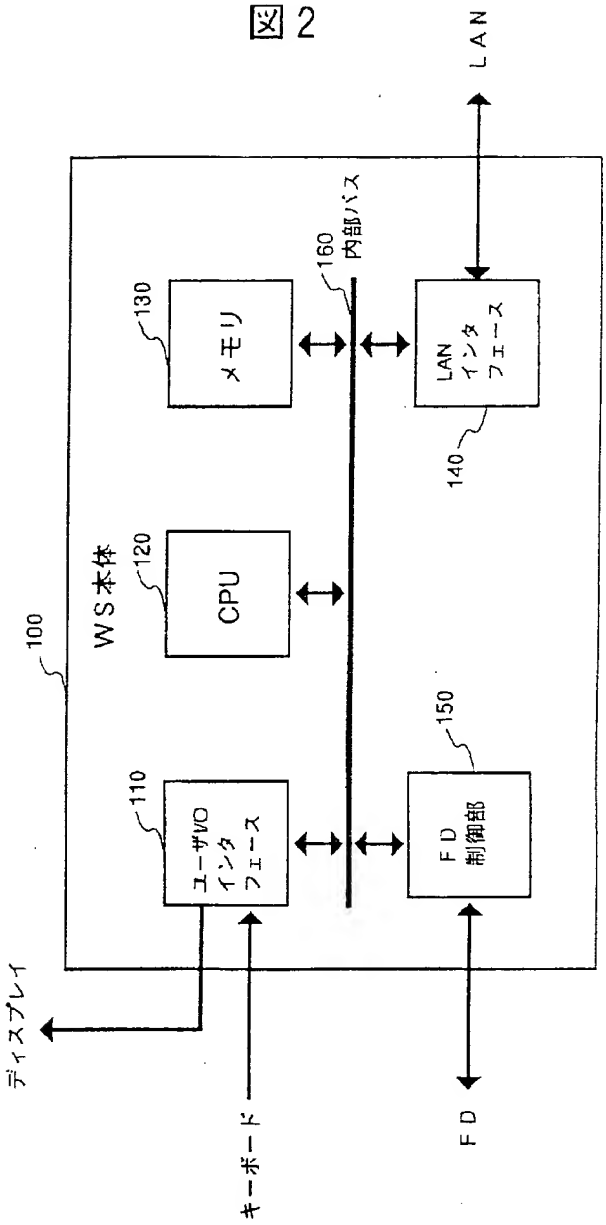
【図1】

図1


伝送部
200
暗号化部
213
メモリ#1
212
暗号化鍵/ID
読み出し回路
216
暗号化鍵ID
挿入回路
215
暗号化回路
214
バッファ
217
暗号化鍵ID
分離回路
220
バッファ
218
解読鍵
読み出し回路
219
メモリ#2
222
メモリ#1
書込制御
211
入力パケット
カウント回路
221
解読回路
223
メモリ#2
書込制御
内部バス
LAN
制御部

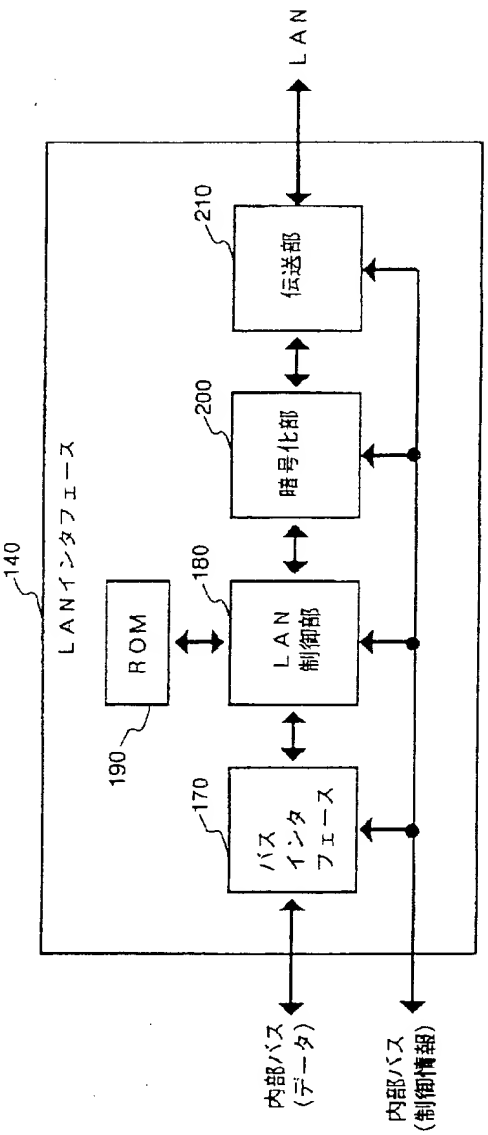
【図2】

図2


LAN
160 内部バス
130 メモリ
LAN インタフェース
140
WS本体
120 CPU
100
110 ユーザI/O インタフェース
150 FD 制御部
ディスプレイ
キーボード
FD

【図3】

図3


LAN
210 伝送部
200 暗号化部
140 LANインタフェース
180 LAN 制御部
ROM
190
170 バス インタフェース
内部バス (データ)
内部バス (制御情報)

【図４】

図４

(a)

301 カウント値	302 暗号化鍵	303 暗号化鍵ＩＤ（Ｈ）
0	C-Key#0	00
1	C-Key#1	01
⋮	⋮	⋮
254	C-Key#254	FE
255	C-Key#255	FF

(b)

401 暗号化鍵ＩＤ（Ｈ）	402 解読鍵
00	D-Key#0
01	D-Key#1
⋮	⋮
FE	D-Key#254
FF	D-Key#255

【図７】

図７

(a)

304 送信パケット宛先アドレス	303 暗号化鍵
DA#0	C-Key#0
DA#1	C-Key#1
⋮	⋮
DA#254	C-Key#254
DA#255	C-Key#255

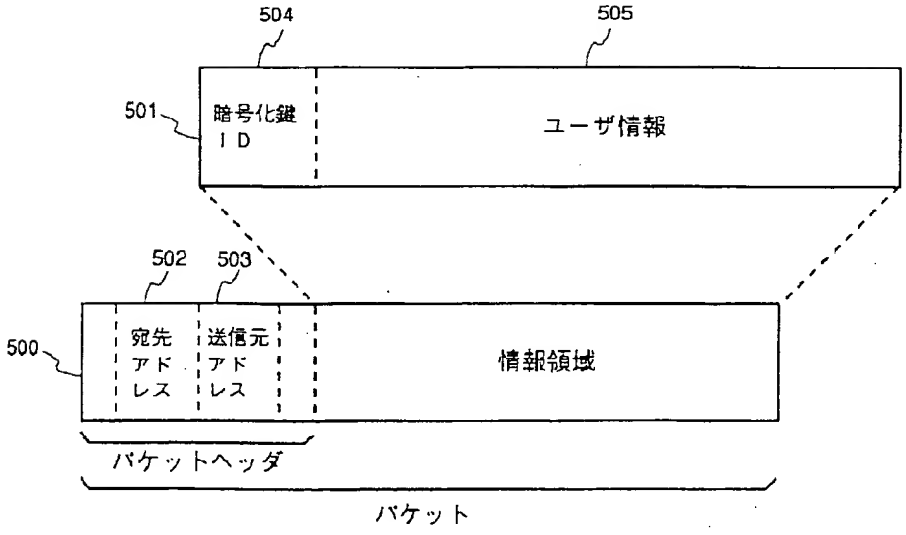
(b)

403 受信パケット宛先アドレス	402 解読鍵
自アドレス	D-Key#X_1
グループアドレス#1	D-Key#X_2
⋮	⋮
グループアドレス#N	D-Key#X_{N+1}
一斉同報アドレス	D-Key#X_{N+2}

但し、$0 \leq X_i \leq 255$ $(1 \leq i \leq N+2)$

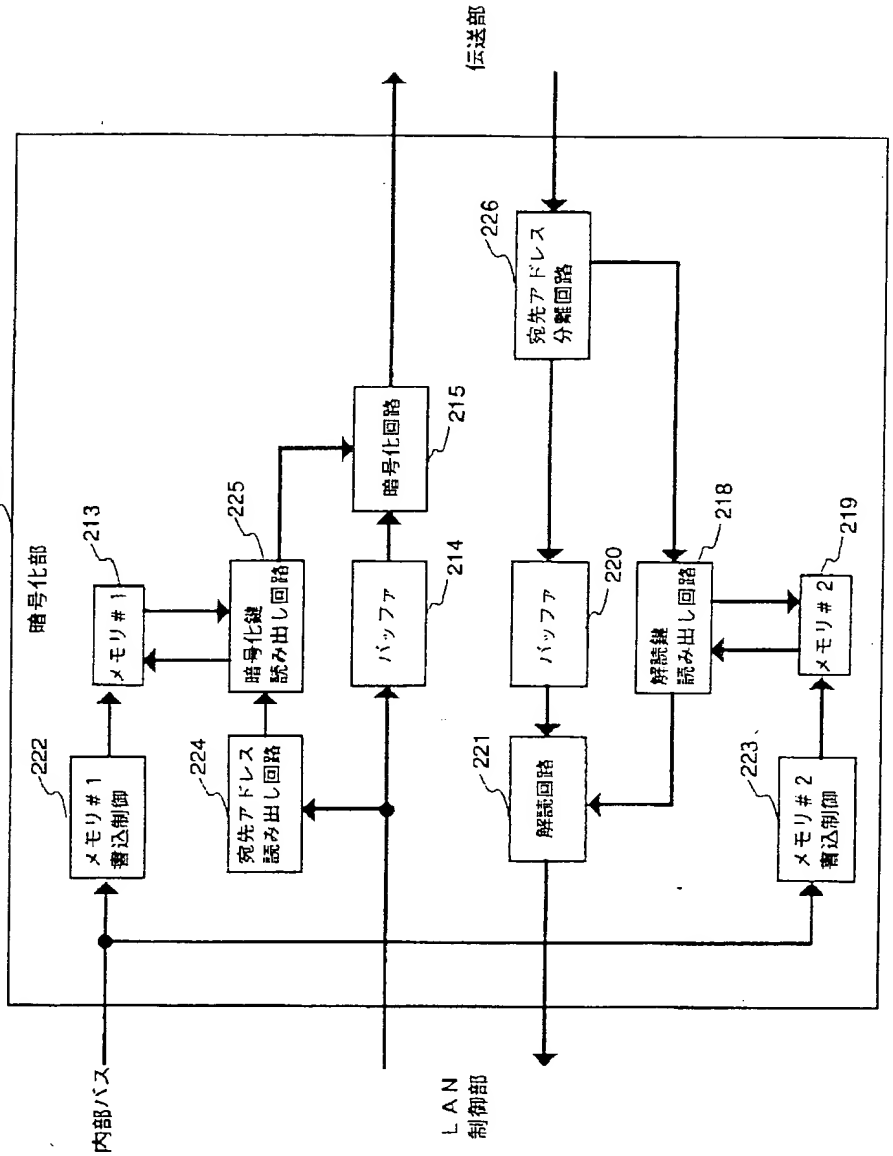
【図５】

図５



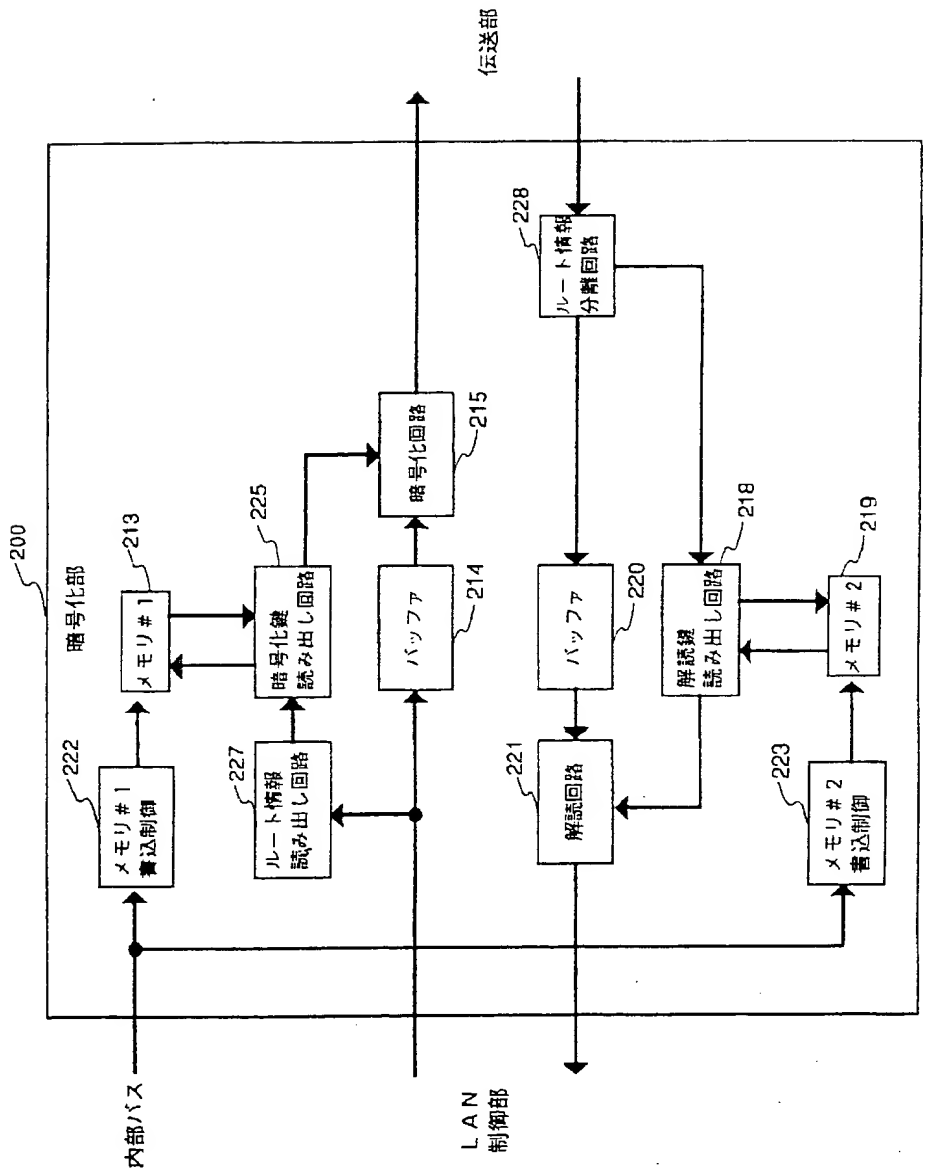
【図6】

図6


200
暗号化部
213
メモリ#1
222
メモリ#1 書込制御
225
暗号化鍵 読み出し回路
224
宛先アドレス 読み出し回路
215
暗号化回路
214
バッファ
内部バス
伝送部
226
宛先アドレス 分離回路
220
バッファ
221
解読回路
218
解読鍵 読み出し回路
219
メモリ#2
223
メモリ#2 書込制御
LAN 制御部

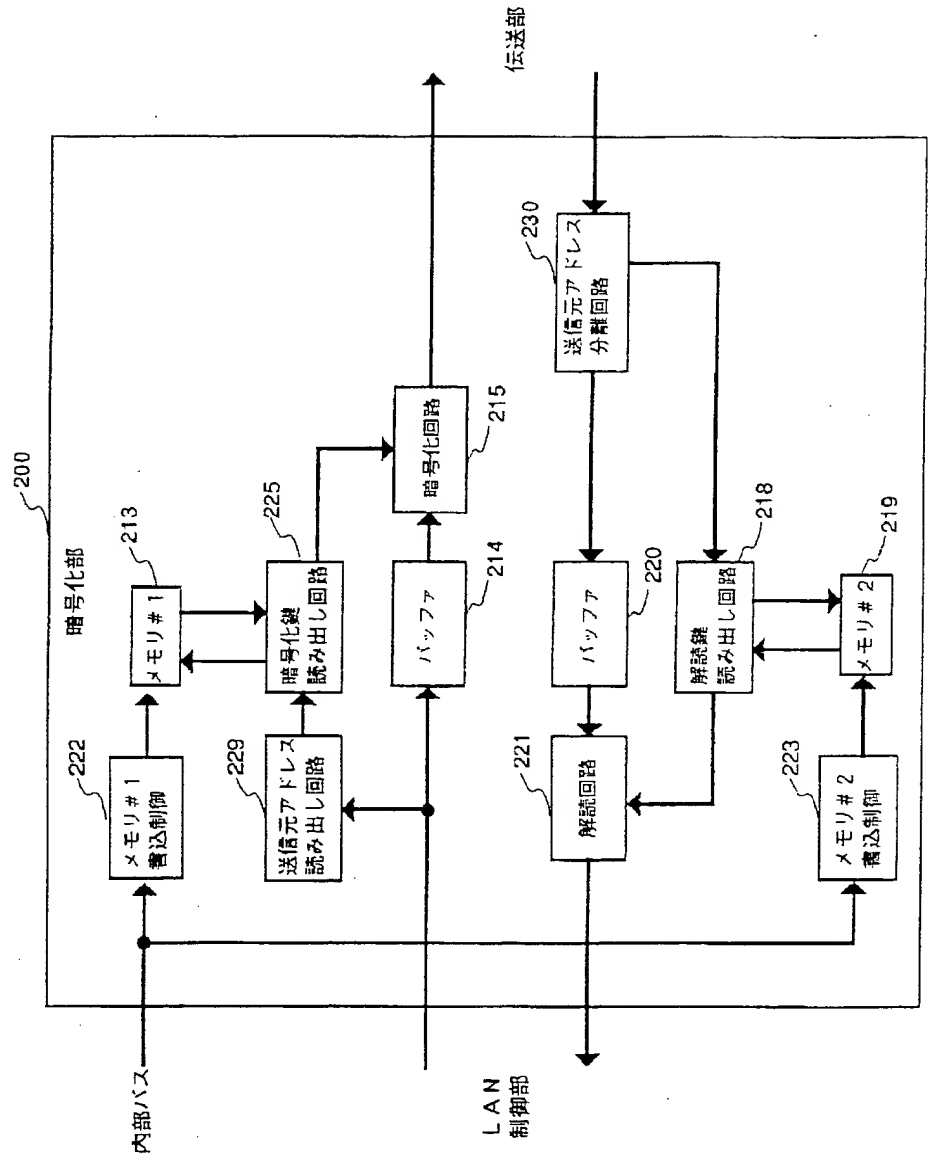
【図8】

図8


伝送部
228
ルート情報
分離回路
200
暗号化部
213
メモリ#1
225
暗号化鍵
読み出し回路
215
暗号化回路
214
バッファ
218
219
メモリ#2
220
バッファ
222
メモリ#1
書込制御
227
ルート情報
読み出し回路
221
解読回路
解読鍵
読み出し回路
223
メモリ#2
書込制御
内部バス
LAN
制御部

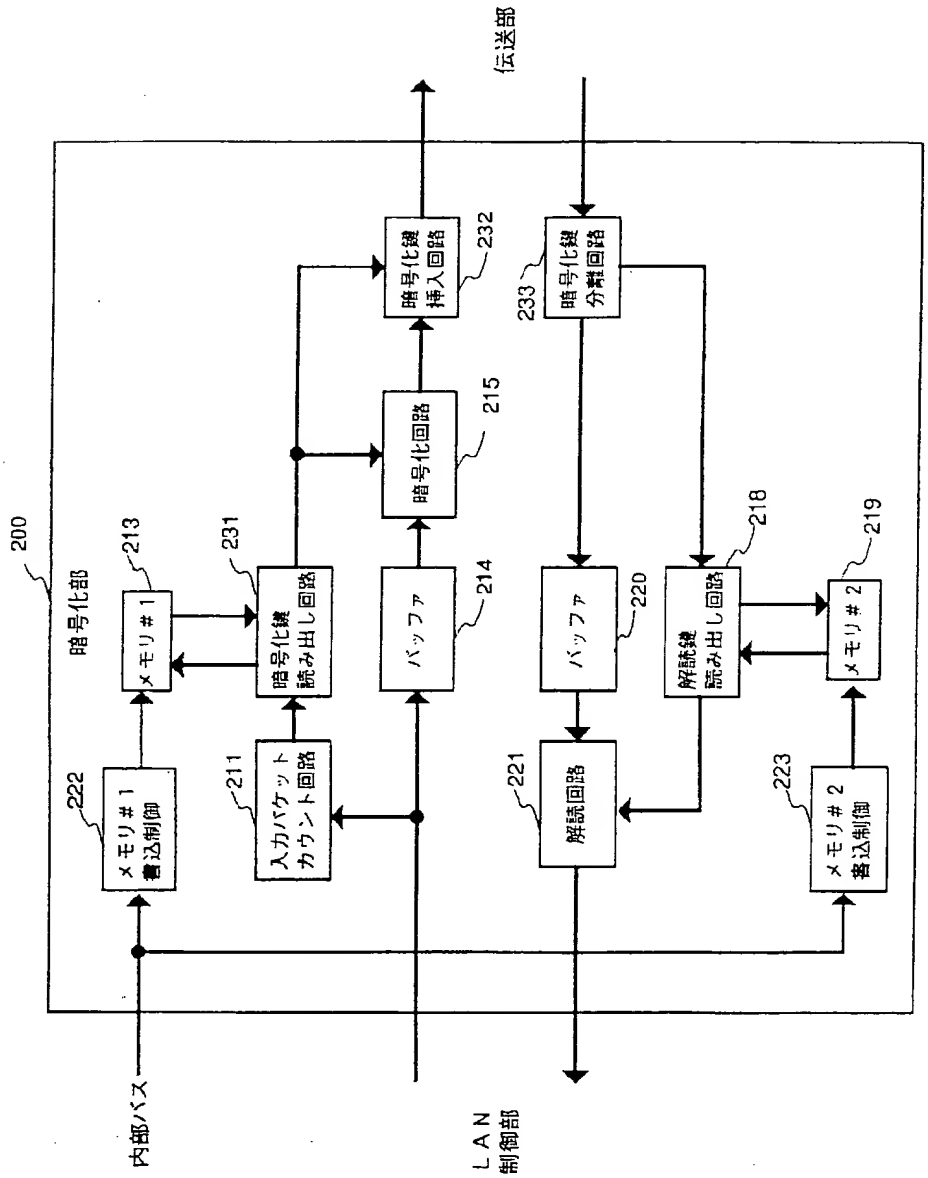
【図10】

図10


200
暗号化部
213
メモリ#1
225
暗号化鍵
読み出し回路
215
暗号化回路
214
バッファ
222
メモリ#1
書込制御
229
送信元アドレス
読み出し回路
内部バス
伝送部
230
送信元アドレス
分離回路
220
バッファ
218
解読鍵
読み出し回路
219
メモリ#2
221
解読回路
223
メモリ#2
書込制御
LAN
制御部

【図１２】

図１２


伝送部
200
暗号化部
213
メモリ＃１
231
暗号化鍵
読み出し回路
232
暗号化鍵
挿入回路
215
暗号化回路
214
バッファ
233
暗号化鍵
分離回路
220
バッファ
218
解読鍵
読み出し回路
219
メモリ＃２
222
メモリ＃１
書込制御
211
入力パケット
カウント回路
221
解読回路
223
メモリ＃２
書込制御
内部バス
ＬＡＮ
制御部

【図13】

図13

(a)

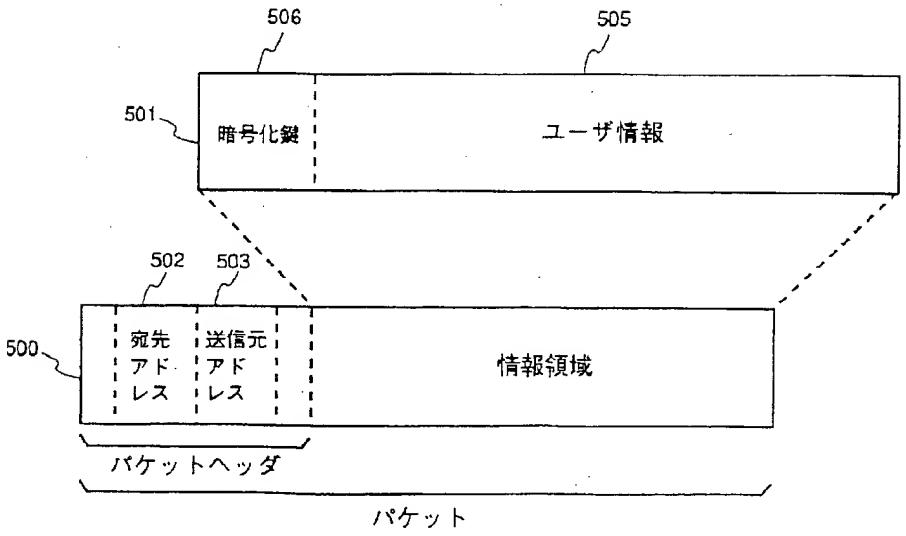
301 カウント値	302 暗号化鍵
0	C-Key#0
1	C-Key#1
⋮	⋮
254	C-Key#254
255	C-Key#255

(b)

406 暗号化鍵	402 解読鍵
C-Key#0	D-Key#0
C-Key#1	D-Key#1
⋮	⋮
C-Key#254	D-Key#254
C-Key#255	D-Key#255

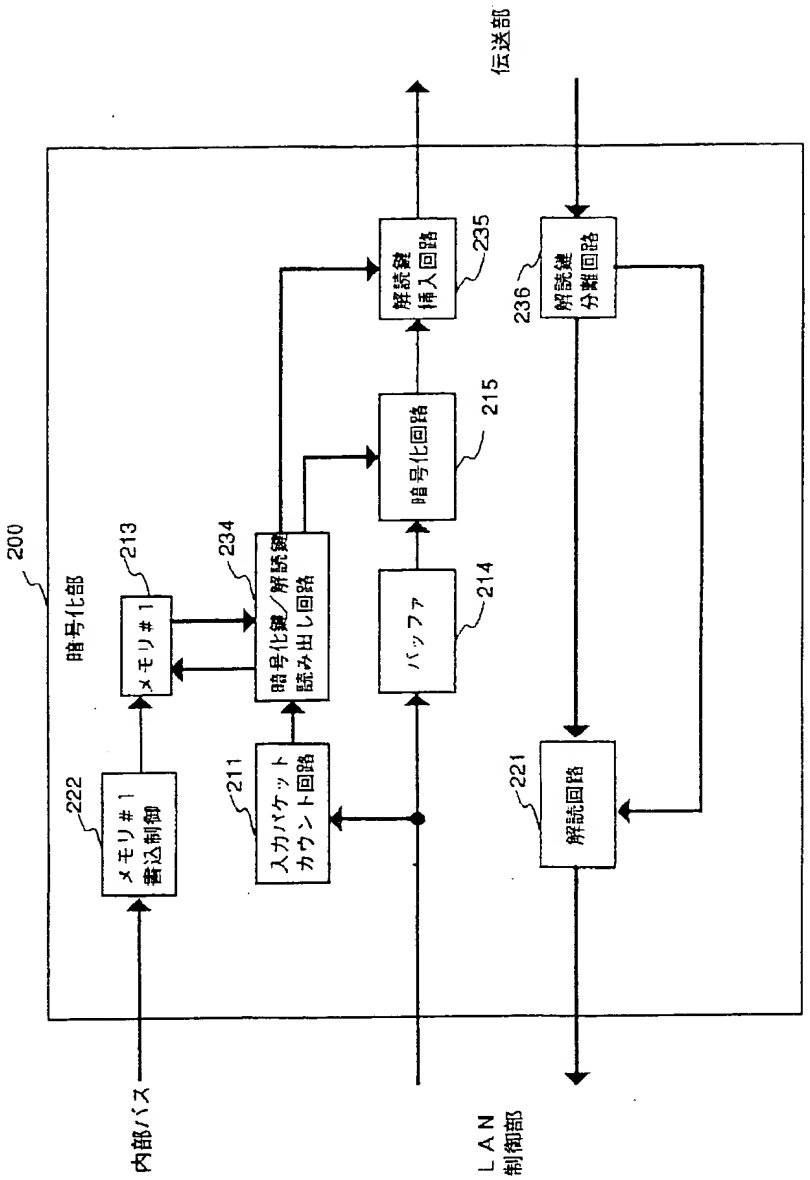
【図14】

図14



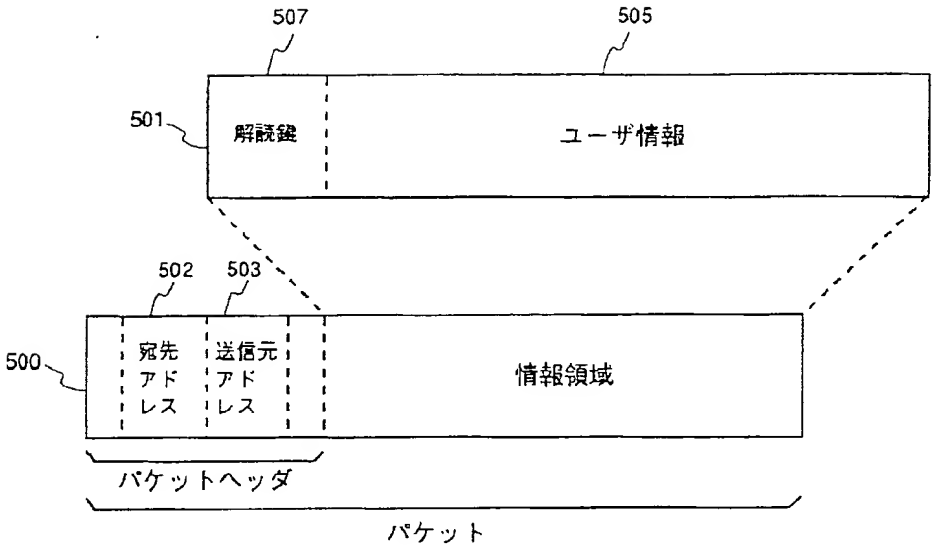
【図15】

図15


伝送部
200
暗号化部
213
メモリ#1
234
暗号化鍵／解読鍵
読み出し回路
235
解読鍵
挿入回路
215
暗号化回路
214
バッファ
236
解読鍵
分離回路
222
メモリ#1
書込制御
211
入力パケット
カウント回路
221
解読回路
内部バス
LAN
制御部

【図１７】

図１７



【図１９】

図１９

(a)

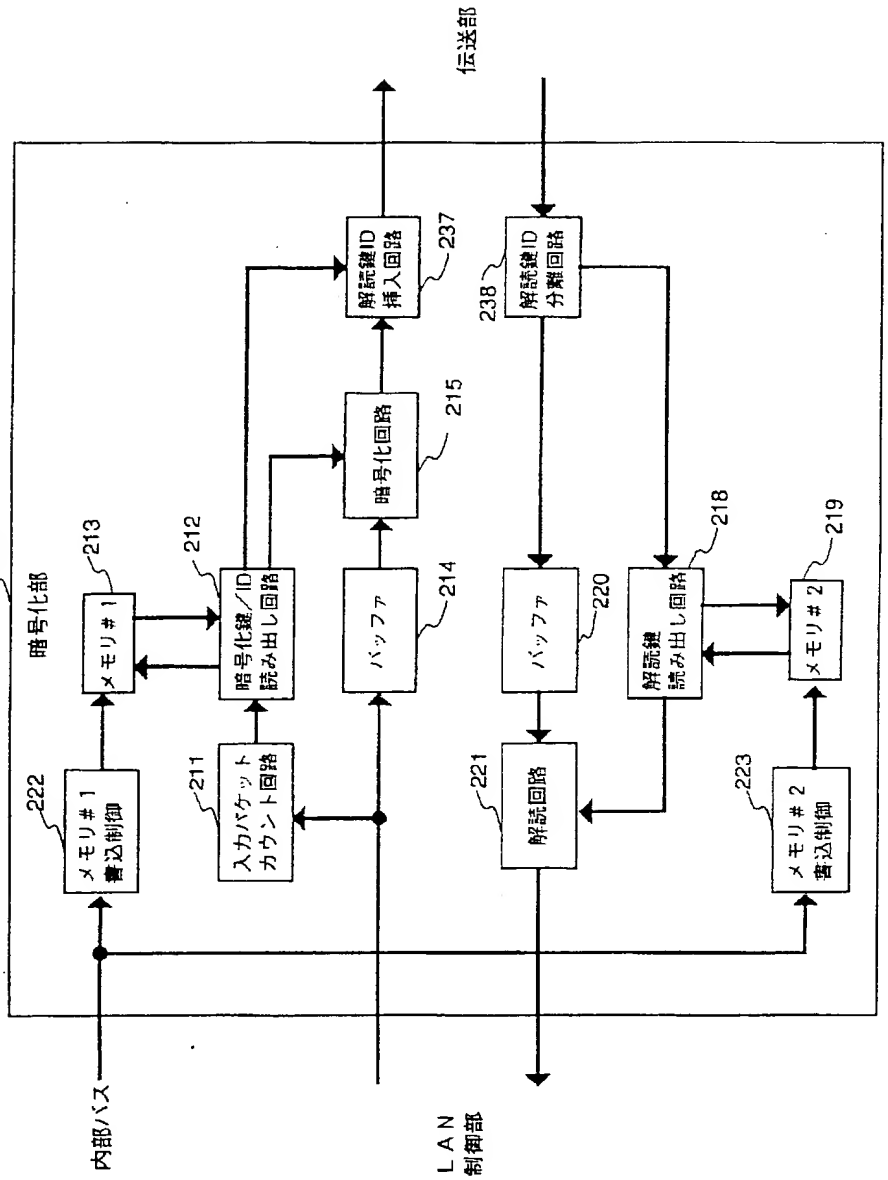
301 カウント値	302 暗号化鍵	308 解読鍵ＩＤ（Ｈ）
0	C-Key#0	00
1	C-Key#1	01
：	：	：
254	C-Key#254	FE
255	C-Key#255	FF

(b)

407 解読鍵ＩＤ（Ｈ）	402 解読鍵
00	D-Key#0
01	D-Key#1
：	：
FE	D-Key#254
FF	D-Key#255

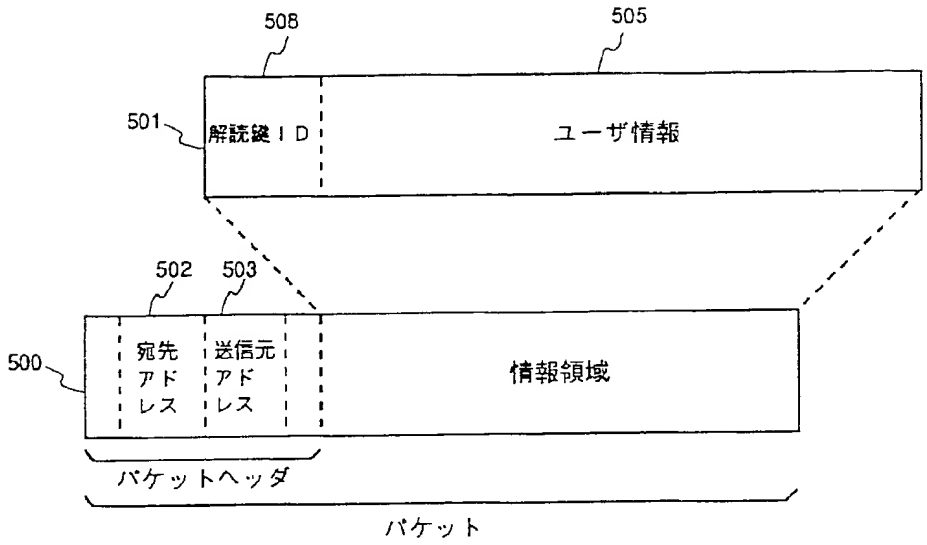
［図１８］

図１８


伝送部
200
暗号化部
213
212
237
238
215
218
219
メモリ＃１
暗号化鍵／ID読み出し回路
解読鍵ID挿入回路
解読鍵ID分離回路
暗号化回路
バッファ
バッファ
解読鍵読み出し回路
メモリ＃２
222
211
221
223
メモリ＃１書込制御
入力パケットカウント回路
解読回路
メモリ＃２書込制御
内部バス
LAN制御部

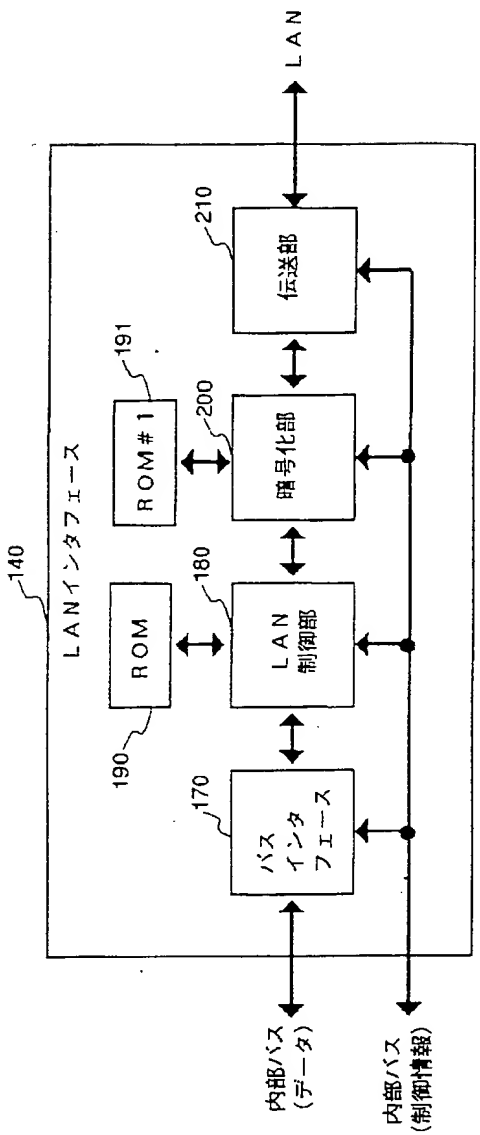
【図２０】

図２０


508
505
501
解読鍵ＩＤ
ユーザ情報
502
503
500
宛先アドレス
送信元アドレス
情報領域
パケットヘッダ
パケット

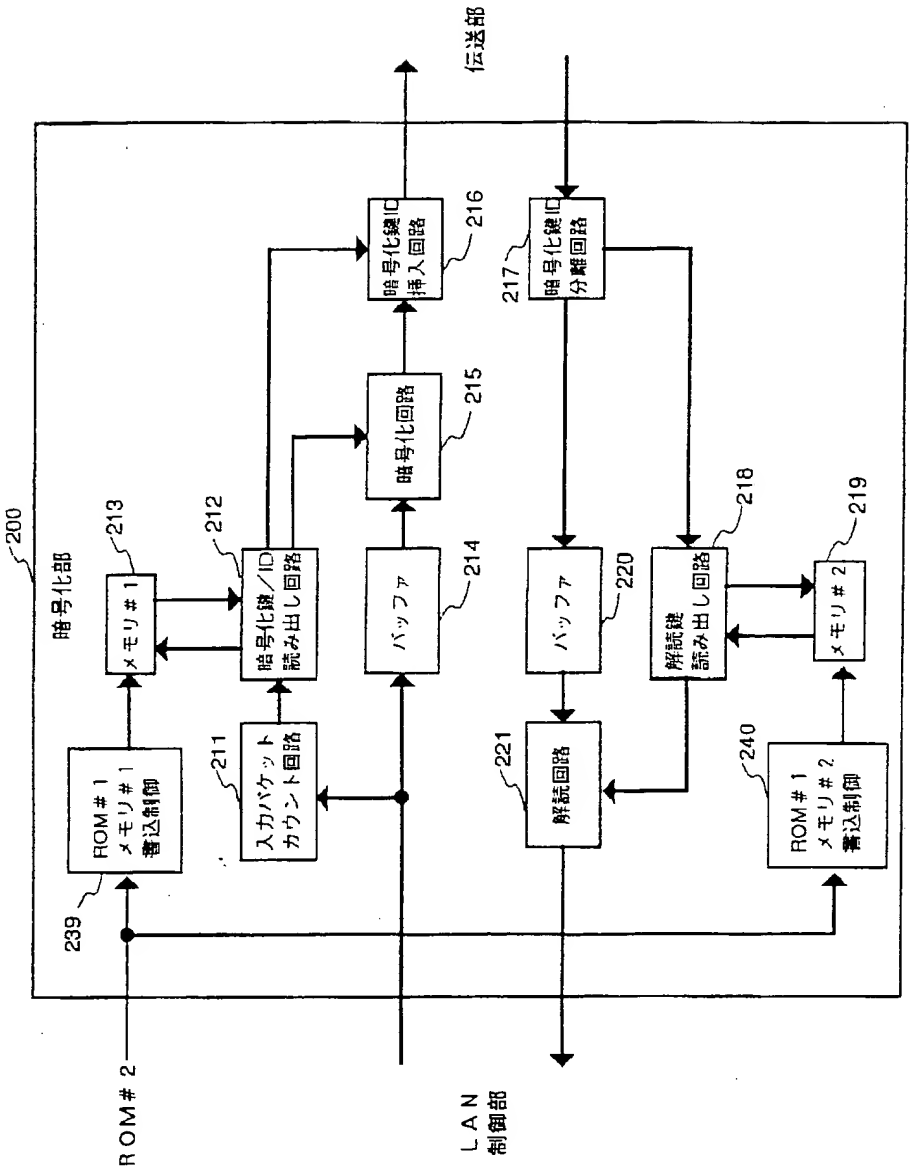
【図21】

図21


LAN
210
伝送部
191
ROM#1
200
暗号化部
140
LANインタフェース
ROM
180
LAN制御部
190
170
バスインタフェース
内部バス（データ）
内部バス（制御情報）

【図２２】

図２２



フロントページの続き

(51)Int.Cl.[5]	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｈ０４Ｌ　12/28				

(72)発明者　鈴木　秀哉
東京都国分寺市東恋ケ窪１丁目280番地
株式会社日立製作所中央研究所内